Information Warfare and International Law

Lawrence T. Greenberg

Seymour E. Goodman

Kevin J. Soo Hoo

National Defense University Press

1998

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1998		**00-00-1998 to 00-00-1998**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Warfare and International Law	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University Press,300 5th Avenue,Fort Lesley J McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**59**	

Table of Contents

Acknowledgments

The authors thank David Alberts of the National Defense University (NDU); John Barton of Stanford Law School; George Bunn of the Stanford University Institute for International Studies; Melanie Greenberg of the Stanford University Center for International Security and Arms Control (CISAC); Daniel Kuehl of the National Defense University; Capt. Richard O'Neill, USN, of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASDC3I); and Edward M. Roche of The Concours Group for their helpful reviews and comments. This work was written under the auspices of the Project on Information Technology and International Security at CISAC, and an earlier version was published as a CISAC Report. We are grateful for the financial, intellectual, and moral support of Dr. Alberts and the Center for Advanced Concepts and Technology of the Institute for National Strategic Studies of the National Defense University, Capt. O'Neill and OASDC3I, and Dr. Michael May of CISAC. We are also grateful for the financial support of the Carnegie Corporation of New York. All errors remain our own.

Preface

National Defense University's Directorate of Advanced Concepts, Technologies and Information Strategies (ACTIS) and School of Information Warfare and Strategy (SIWS) are pleased to inaugurate a new series of publications by the National Defense University Press intended to explore the evolving relationship between the law and information warfare. The emerging debate over information warfare and the information component of national power has frequently emphasized technological issues with scant regard for the legal environment in which the Information Age is occurring, yet this may obscure some very real and unsettling legal issues that will have to be solved in order to wage information warfare. One of the persistent trends in the related histories of the law and warfare is that whenever war, or civil society in general, has extended into a new environment, such as underwater or the aerospace, the law has had to "play catch-up" to the technology. This should be no surprise: after all, no one writes law for something that does not exist, such as aerial warfare before the invention of the airplane. The same is true for cyberspace, which is why many argue that the legal environment for information warfare is even less well framed than the technology making it possible. To the theater campaign or operations planner who must wrestle with "here and now" issues regarding the use of information warfare and protection from the enemy's potential use of it, theoretical discussions of information warfare and the law are a thin gruel when weighed against the need for firm guidelines, rules of engagement, and policy.

When one begins to examine the relationship between information warfare and the law, especially international law and the law of war, it immediately becomes apparent that some fundamental questions need to be explored. What, for example, is war in the Information Age, and what types of activities between information actors, whether nation states or non-state entities, will we call information warfare? What is an "act of (information) warfare," to use that imprecise but expressive and widely used term? What is "war" in the Information Age? Who is a "combatant"? What are "force," "armed

attack," or "armed aggression" (terms from the UN Charter) in the Information Age, and do they automatically equate to IW? Does "war" between states require physical violence, kinetic energy, and human casualties? What role is played by intent? How might the law itself change in response to the Information Age? How will long-established legal principles such as national sovereignty and the inviolability of national boundaries be affected by the ability of cyberspace to transcend such concepts? Will the technologies of the Information Age, by bringing atrocities and violations of the law of war into the intense and immediate glare of global public awareness, increase the observance of the legal norms of armed conflict? Information warfare also raises specific legal issues related to computer crime: what is a crime, who commits it, and what does the law say about it? These questions and issues merely hint at the tremendous uncertainties that surround the evolving discipline of information warfare and field of national and global information power.

This series of publications is intended to provide a context within which to examine IW in a legal sense and explore specific issues such as the laws of war or standing international agreements to which the United States is a signatory, such as the International Telecommunications Union or the UN Charter. This initial monograph, by Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, is an outstanding kickoff to this series. The authors, members of the Project on Information Technology and International Security at Stanford University's Center for International Security and Arms Control, have surfaced and explored some profound issues that will shape the legal context within which information warfare may be waged and national information power exerted in the coming years. They note that despite the newness of both the technology of IW and the evolving concepts for its employment, legal constraints will almost certainly apply to IW. Also noting that concepts of sovereignty based on physical territoriality do not function well in cyberspace, the authors observe that there is no authoritative legal or international agreement as to whether an IW "attack" equals an "attack" or "use of force" in the traditional sense. With this as a context, the authors offer several legal approaches the United States could employ to protect the national information infrastructure or clarify options useful for offense, defense, or retaliation. They are under no illusions that they have answered all of the questions relating to information warfare and international law, but rather can take great satisfaction in having cogently and thoroughly explored key legal questions and issues that information warriors, jurists, and policy makers will wrestle with in the future. In doing so they have made a significant and lasting contribution to national and international security, stability, and peace.

Daniel T. Kuehl, Ph.D
Professor, School of Information Warfare & Strategy
Series General Editor

Executive Summary

The development of "information warfare" presents international legal issues that will complicate nations' efforts both to execute and to respond to certain information warfare attacks, specifically those using computers, telecommunications, or networks to attack adversary information systems. Some legal constraints will certainly apply to information warfare, either because the constraints explicitly regulate particular actions, or because more general principles of international law govern the effects of those actions. Nevertheless, the novelty of certain information warfare techniques may remove them from application of established legal categories. Furthermore, the ability of signals to travel across international networks and affect systems in distant countries conflicts with the longstanding principle of national, territorial sovereignty.

First, it has not been established that information attacks, particularly when they are not directly lethal or physically destructive, constitute the use of "force" or "armed attack" under such provisions as the United Nations Charter. Such attacks thus may be legal forms of coercion even in peacetime, and the use of conventional armed force may not be an appropriate response to such attacks; indeed, such a response might be considered an act of aggression. No provision of international law prevents countries from taking many actions against other states, such as embargoes, that inflict great hardship on those states and their populations. Second, it is equally unclear whether some of the damage that information warfare attacks could inflict, as by disrupting government or private databases and systems, is the sort of damage that international humanitarian law is intended to restrain. Finally, where attacks can be executed across international networks, the United States (among others) may need to rely upon foreign assistance in identifying and responding to those who have attacked it.

The ambiguous state of international law regarding information warfare may leave space for the United States to pursue information warfare activities. Conversely, it may permit adversaries to attack the United States and its systems. When considering policy options, U.S. decision makers must balance those offensive opportunities against defensive vulnerabilities, a balance that is beyond the scope of this report. Nevertheless, we can discuss several, nonexclusive international legal approaches that the United States may pursue to protect its systems or clarify its offensive, defensive, and retaliatory options.

First, the United States could pursue international definitions of such concepts as "force" or "armed attack" as they apply to information warfare; such definitions could help establish when such attacks can be conducted and how countries may respond to them. Second, the United States could pursue international cooperation against information warfare attacks, encouraging cooperation in the investigation and prosecution of those responsible for the attacks, particularly terrorists and other criminals. Third, the United States may pursue agreements to protect critical information systems, either by putting them off limits for legitimate attacks, or creating international protection regimes for particular systems. Fourth, some have suggested that information warfare may be an appropriate area for arms control agreements. However, several factors, including the novelty of many information warfare technologies and techniques, the wide dissemination, small size, and predominantly civilian nature of much information

technology, and the danger that arms control would not apply to non-state actors, such as terrorists, all suggest that the pursuit of arms control would be premature at best, especially in connection to largely nonlethal technologies in which the United States apparently leads other nations. Despite the apparent attractiveness of taking legal measures to either protect U.S. systems or preserve the availability of information weapons for U.S. use, law may not be nimble enough to keep up with technological change, and thus will not be a substitute for vigilance, preparedness, and ingenuity.

Chapter 1: Introduction

The Development of Information Warfare

As the worldwide explosion of information technology, including computing, telecommunications, and networks, is changing the way we conduct business, government, and education, it promises to change the way we fight.[1] Information technology is diffusing into virtually all military weapons, communications, and command and control systems, as well as the civilian systems that support modern industrial (or post-industrial) economies and their military efforts. Some of the new ways of fighting have been labeled "information warfare," which has been broadly defined as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[2] As such, information warfare includes both new techniques, such as computer intrusion and disruption and telecommunications spoofing, and old ones, such as ruses, camouflage, and physical attacks on observation posts and lines of communication. Some have suggested that information warfare could usher in an era of largely bloodless conflict; battle would occur in "cyberspace," as U.S. "information warriors" would be able to disable important enemy command and control or civilian infrastructure systems with little, if any, loss of life.[3] Others have projected futures of conflict in which the bloodletting is only enhanced by improved and broadened communications.[4] Still others have suggested that information technology may contribute to the development of new forms of social organization, along with new forms of conflict.[5]

Whatever the development and diffusion of information technology mean for the future of warfare, it is apparent that some of the new forms of attack that information technology enables may be qualitatively different from prior forms of attack. The use of such tools as computer intrusion and computer viruses, for example, may take war out of the physical, kinetic world and bring it into an intangible, electronic one. These newer forms of attacks, some of which may seem to be the products of science fiction, range along continuums extending from those with no physical impact on the enemy to some that would cause grave destruction or loss of life, from those with no physical intrusion beyond national borders to those requiring traditional, military invasions, and from those affecting purely civilian targets to those hitting purely military ones. Attacks could be conducted from a distance, through radio waves or international communications networks, with no physical intrusion beyond enemy borders. Damage could range from military or civilian deaths from system malfunctions, to the denial of service of important military or governmental systems in time of crisis, to widespread fear, economic hardship, or merely inconvenience for civilian populations who depend upon information systems in their daily lives.

The following are examples-some likely, some perhaps farfetched-of attacks that countries or nongovernmental entities might pursue, or suffer, as they wage warfare in the Information Age.

- A "trap door" might be hidden in the code controlling switching centers of the Public Switched Network, causing portions of it to fail on command.[6]

- A mass dialing attack by personal computers might overwhelm a local phone system.[7]

- A "logic bomb" or other intrusion into rail computer systems might cause trains to be misrouted and, perhaps, crash.[8]

- An enemy's radio and television network might be taken over electronically, and then used to broadcast propaganda or other information.[9] Advanced techniques such as "video morphing" could make the new broadcasts indistinguishable from the enemy's own usual broadcasts.[10]

- A computer intruder might remotely alter the formulas of medication at pharmaceutical manufacturers, or personal medical information, such as blood type, in medical databases.[11]

- A concerted e-mail attack might overwhelm or paralyze a significant network.[12]

- Computer intruders might divert funds from bank computers, or corrupt data in bank databases, causing disruption or panic as banks need to shut down to address their problems.[13]

- Computer intruders might steal and disclose confidential personal, medical, or financial information, as a tool of blackmail, extortion, or to cause widespread social disruption or embarrassment.

- A "computer worm" or "virus" could travel from computer to computer across a network, damaging data and disrupting systems.[14]

- An "infoblockade" could permit little or no electronic information to enter or leave a nation's borders.[15]

- A nation's command and control infrastructure could be disrupted, with individual military units unable to communicate with each other, or with a central command.

- Stock or commodity exchanges, electric power grids and municipal traffic control systems, and, as is frequently suggested, air traffic control or navigation systems could be manipulated or disrupted, with accompanying economic or societal disruption, physical destruction, or loss of life.[16]

International Law

The Law of Nations

Law attempts to govern war, as it does most human endeavors. International law governs interaction among nations. International law primarily consists of "conventional" law and

"customary" law.[17] Conventional law is that made by treaty or other explicit agreement among nations, who are bound to their agreements under the principle of pacta sunt servanda, or "agreements are to be observed."[18] Examples of conventional law would include the Paris Peace Treaty of 1783, which ended the U.S. War of Independence and fixed the borders of the new republic, the 1968 Treaty on the Non-Proliferation of Nuclear Weapons, and the General Agreement on Tariffs and Trade (GATT).

Customary law results from the general and consistent practice of states' opinio juris, or with the understanding that the practice is required by law, not just expedience. Customary law may develop from understandings reflected in treaties or other agreements, even if they have not been ratified, declarations or votes of international bodies such as the General Assembly of the United Nations, or the statements and actions of governments and their officials.[19] There is no universally accepted way to determine whether a customary international legal norm has been established. To a great extent, customary international law must be like obscenity to the late U.S. Supreme Court Justice Potter Stewart-something we know when we see it.[20] Examples of customary law include the traditional protected status of diplomats and the historical three-nautical mile claim to coastal territorial waters.

Even when legal norms seem well-established in theory, patterns of contrary state practice may contribute to the decline or alteration of the principles. Just as popular disregard for a trademark, such as cellophane, aspirin, or thermos, can result in that trademark losing its legal force and becoming a generic term, violation of an ostensible customary legal principle can cause its demise.[21] Law based upon actors' recognition that it is indeed law loses force when those actors no longer recognize it.[22]

In considering international law, particularly in the context of national security, it is important to stress some distinctions between international and domestic law. Unlike most nations' domestic law, international law is not a body of law created by legislatures and courts and enforced by police through a court system. Rather, international law is generally established by agreement, either explicit or tacit, among the parties who will be bound by it, much as private parties enter into contracts with each other. Although international legal forums, such as the International Court of Justice, do exist, their enforcement mechanisms are limited at best; no international police force walks the world beat. Consequently, a country that is willing to accept the political and diplomatic consequences that may ensue when it defies international law may do so. As a crude example, the Revolutionary Islamic government of Iran blatantly disregarded the traditional sovereignty and sanctuary of the U.S. Embassy in Tehran in the late 1970s and early 1980s, but if it had any concerns about external reactions, those concerns seemed more directed at the threat of economic sanctions or U.S. military action, not at some global police force. It seems likely that nations will be least likely to follow the dictates of international law where those dictates endanger or conflict with the pursuit of their fundamental interests, including national security.

The Legal Challenges of Information Warfare

From a legal perspective, the older forms of information warfare pose few unanswered questions under customary or treaty law. For example, the use of camouflage to elude

enemy observers was old even when Macduff and his men brought Burnham Wood to Dunsinane;[23] ancient Greek soldiers blinded their foes by reflecting the sun off their shields; and both sides attempted to cut each others' telegraph lines during the U.S. Civil War, and there is little doubt of these actions' propriety. Similarly, wartime physical attacks against military observation systems, from lookout posts to radar stations, are unquestionably acceptable under international law.

But the development of information technology, specifically computers, telecommunications, and networks, makes it possible for adversaries to attack each other in new ways and with new forms of damage, and may create new targets for attack. Attackers may use international networks to damage or disrupt enemy systems, without ever physically entering the enemy's country, and countries' dependence upon electronic or other information-based systems may make those systems particularly attractive targets. Furthermore, the dual-use nature of many information systems and infrastructures may blur the distinction between military and civilian targets.

Such new attacks may pose problems for international law because law is inherently conservative; technological change may enable new activities that do not fit within existing legal categories, or may reveal contradictions among existing legal principles. Information warfare challenges existing international law in three primary ways. First, the sort of intangible damage that such attacks may cause may be analytically different from the physical damage caused by traditional warfare. The kind of destruction that bombs and bullets cause is easy to see and understand, and fits well within longstanding views of what war means. In contrast, the disruption of information systems, including the corruption or manipulation of stored or transmitted data, may cause intangible damage, such as disruption of civil society or government services that may be more closely equivalent to activities such as economic sanctions that may be undertaken in times of peace.

Second, the ability of signals to travel across international networks or through the atmosphere as radio waves challenges the concept of national, territorial sovereignty. Sovereignty, which has been a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each nation has exclusive authority over events within its borders.[24] Sovereignty may not be suited to an increasingly networked, or "wired" world, as signals traveling across networks or as electromagnetic waves may cross international borders quickly and with impunity, allowing individuals or groups to affect systems across the globe, while national legal authority generally stops at those same borders. Furthermore, the intangible violation of borders that signals may cause may not be the sort of violation traditionally understood to be part of a military attack.

Third, just as information warfare attacks may be difficult to define as "peace" or "war," it may be hard to define their targets as military (and thus generally legitimate targets) or civilian (generally forbidden). Furthermore, the intangible damage the attacks cause may not be the sort of injuries against which the humanitarian law of war is designed to protect noncombatants.

Graphic representations may be helpful in understanding the analytical continuums along which information attacks may occur. Figure 1 illustrates the physical destructiveness of attacks, ranging from a propaganda broadcast, which may have no physical effects on its target, to a computer intrusion that may hinder the workings of government, military or civilian systems, to a computer intrusion that causes a destructive or fatal system failure. Most physically destructive, of course, would be an attack using massive kinetic force, with a thermonuclear attack as an extreme example. It is not difficult to place attacks along the continuum in a manner that is not quite arbitrary, although the appropriateness of each particular point may be debatable. It may be much harder to establish the location of the point on the continuum that divides "peace" from "war," or to determine when each particular attack may be permissible under international law.[25]

FIGURE 1

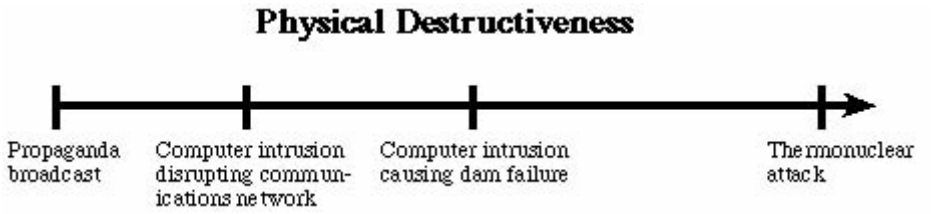


Figure 2 illustrates the extent to which particular attacks intrude across nations' borders. Least intrusive would be an "infoblockade," whereby a country's communications beyond its borders would be cut off.[26] A computer intrusion might be considered to violate the target country's borders, whatever its destructive impact, although such characterization may not be inevitable, as discussed in Part II. Espionage, with the infiltration of an agent into the target country, would obviously require the crossing of borders, although perhaps on a limited scale. Finally, a military invasion's intrusiveness is obvious. Just as the destructiveness of an attack may be relevant for its characterization as "peace" or "war," so too will be this element of intrusion across borders, with the potential difference that it may be easier to characterize the destructiveness of an attack than it may be to determine the extent to which an attack violates a nation's borders (and sovereignty).[27]

FIGURE 2

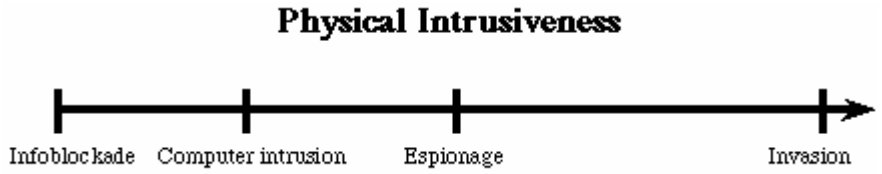
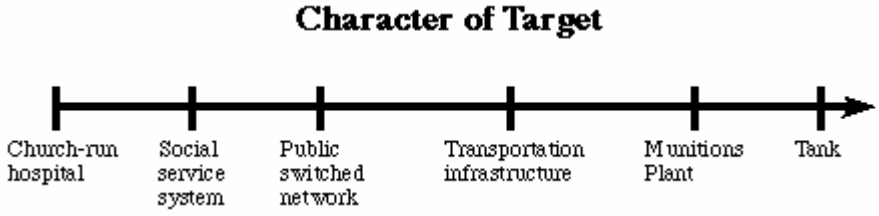


Figure 3 illustrates the diverse character of the targets of potential attacks. Some targets, such as armored forces on the battlefield, are unambiguously military in character, and are thus the legitimate targets for attacks. Other targets, such as churches, kindergartens, or hospitals, are purely civilian in character, and may not be made the targets for attacks, although they may often suffer collateral damage from otherwise legitimate attacks. The acceptability of other targets, ranging from government social service systems to munitions factories, may vary with their contribution to a nation's war effort. As

discussed, the dual-use nature of many telecommunications and computing systems may make them subject to attacks that will have grave civilian consequences. The borderline between legitimate and illegitimate targets of war is thus difficult to draw in the abstract. Furthermore, information warfare techniques that may cause grave hardship to civilians may not be considered to be "war," and may not be covered by the humanitarian provisions that attempt to lessen war's cruelty.[28]

FIGURE 3



The Purpose of This Book

The Importance of International Law for U.S. Policy

The United States has a particularly significant stake in understanding how international law will apply to these new forms of conflict. First, as a matter of domestic politics, the United States has a largely legal culture. The U.S. Government is described as one of laws; in public political rhetoric acts are routinely described and discussed in legal terms, and characterizing an act as illegal can be a harsh and politically damaging criticism. Second, as a matter of domestic law, international law is as much a part of the "law of the land" as are the statutes that Congress enacts.[29] Third, given the U.S. Government's apparent preference in the post-Cold War era (and even before) for acting militarily under the auspices of international coalitions or the United Nations, its prospects for obtaining such auspices are greater when it can persuade other nations that its actions are legal and those of its foes are not. Finally, as the preeminent world power, and one particularly dependent upon information systems, the United States has a stake in the international status quo. To the extent international law helps to provide stability and protect critical information systems, it may benefit U.S. interests.

The Scope of This Book

This book will identify issues that arise from the development of information warfare under international law, and discuss how the law might be applied.[30] It will look at both offensive information warfare and the responses that a nation may make to attacks on its information systems. Finally, the book will outline approaches to resolving legal ambiguities surrounding information warfare and addressing some of the difficulties that arise when old laws and new technologies collide.

Chapter 2: The Conduct of Information Warfare and International Law

The Legality of Information Warfare

Perhaps because of the newness of much of the technology involved, no provision of international law explicitly prohibits what we now know as information warfare. This absence of prohibitions is significant because, as a crudely general rule, that which international law does not prohibit it permits.[31] But the absence is not dispositive, because even where international law does not purport to address particular weapons or technologies, its general principles may apply to the use of those weapons and technologies.[32] Nevertheless, existing international law leaves space for many types of information warfare techniques in many circumstances.

International Telecommunications Law

Any attack involving networks and telecommunications may implicate the International Telecommunication Union (ITU) and its underlying charter, the International Telecommunication Convention (ITC), which apply to international wire and radio frequency communications.[33] In practice, the ITU may not substantially limit information warfare activities, particularly by the United States and especially in a wartime context.

The primary concerns of the ITU are interoperability and interference.[34] Its predecessor organization, the International Telegraph Union, was established in 1865 to facilitate international telegraph traffic, mainly within Europe.[35] One of the Union's early sets of regulations for radio required interoperability of maritime radio systems, after several dangerous naval incidents occurred because the Marconi Wireless Company, which held the exclusive right to install and operate shipboard radio equipment, refused to permit its operators to communicate with any station that did not use Marconi equipment.[36]

The ITU and the regulations promulgated under it do have some applicability to information warfare attacks that use the electromagnetic spectrum or international telecommunication networks. First, broadcasting stations from one nation may not interfere with broadcasts of other states' services on their authorized frequencies.[37] The International Frequency Regulation Board (IFRB) of the ITU allocates the electromagnetic spectrum to prevent interference.[38] Even military installations must observe the noninterference requirement.[39] Additionally, offshore radio stations are banned, [40] and states may not carry out the transmission of false or misleading signals.[41] Finally, governments must protect the secrecy of international correspondence,[42] although they retain the right to stop radio or wire transmissions for national or domestic security purposes.[43]

The aforementioned provisions would seem to block the disruption or spoofing of adversaries' telecommunications, but in practice they may not. First, the rules against interference do not apply between belligerents, so wartime communications are fair game.[44] Secondly, even in peacetime, violation of the ITU rules and regulations may have limited repercussions, especially for a country as significant in international

telecommunications as the United States. The IFRB is more of a coordinating body than a regulatory agency,[45] and it has no actual authority to enforce its decisions; rather, countries respect its edicts against interference so that their own communications will be similarly protected.[46] Even if international sanctions appeared likely, the United States might decide that the risks it faced from external interference would not outweigh its need to conduct operations against a particular adversary. Finally, it is important to note that even where information warfare activities do violate the ITU or its regulations, mere violations are more likely to be considered breaches of contractual obligations under treaty than acts of war justifying forceful responses.[47]

Interestingly, the Charter of the United Nations, drafted 50 years ago, appears to contemplate such interference with a country's communications as "infoblockades." Article 41 provides that in its effort to address breaches of the peace, the UN Security Council may call upon UN members to disrupt an aggressor's "rail, sea, air, postal, telegraphic, radio, and other means of communication."

Space

Because of the importance of satellites for international telecommunications, as well as for military (especially U.S.) command, control, communications, and intelligence, many information warfare attacks (including jamming or spoofing of communications or efforts to overcome them) may involve orbital assets, and thus implicate space law. Space law, though, leaves ample room for information warfare.

The fundamental document of space law, the multilateral 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (the "Outer Space Treaty"), provides that all states shall be free to explore and use outer space on a basis of equality and that no state may place into Earth orbit any objects carrying nuclear weapons or any other kind of "weapon of mass destruction."[48] The 1979 Agreement Concerning the Activities of States on the Moon and Other Celestial Bodies (the "Moon Treaty") applies similar prohibitions to the moon,[49] and also states that the moon shall only be used for peaceful purposes.[50] The 1971 Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT)[51] and the 1976 Convention on the International Maritime Satellite Organization (INMARSAT)[52] also affect telecommunications and the use of space, but their relevance is limited to principles of nondiscrimination among nations using the relevant satellites.

None of these conventions bars information warfare activities that make use of satellite assets.[53] First, although some might argue that state practice and such agreements as the Moon Treaty have created a legal norm of peaceful use of outer space or the avoidance of orbital arms races,[54] it is unquestionable that space can be, and has been, used for military purposes. Orbital surveillance is legal and common,[55] and space is routinely used for military communications, navigation, and weapons guidance. In any event, the meaning of "peaceful use" of outer space is unsettled,[56] and, with its often nonlethal, physically nonintrusive character, it is possible that much of "information warfare" could be considered "peaceful."[57]

Second, for the Outer Space Treaty's prohibition against orbital weapons of mass destruction to apply, it would first have to be determined that the weapons used in an information warfare attack, particularly an electronically based one, were weapons of mass destruction.[58] Many information warfare attacks, which may have no direct physical effects, cannot easily be considered to cause mass destruction in the same way as would, say, an atomic bomb. Furthermore, assuming that the weapons of information warfare could constitute "weapons of mass destruction," those weapons, even when they use satellites, might not be considered to be in space. For example, when a satellite is used to transmit a signal for computer intrusion or sabotage or in communications spoofing, the ultimate "weapon of mass destruction" (the originator of the signal) may actually be on the ground, and the satellite only a conduit for the attack, just as satellites used for guidance of intercontinental ballistic missiles would not be "weapons of mass destruction."[59]

State Practice

State practice, itself a major source of customary international law,[60] seems to permit much of what would go into information warfare. First, espionage, although universally criminal under domestic laws, does not, by itself, violate international law.[61] Furthermore, orbital remote sensing, which may include the bombardment of a country's territory with radar or other forms of electromagnetic radiation, is permissible during war or peace.[62]

Second, an adversary's communications are recognized as legitimate targets for disruption during war. Undersea cables, including those connecting belligerents with neutrals, have been interfered with during all naval wars since the Spanish-American War, as Article 15 of the 1884 Convention for the Protection of Undersea Cables exempts belligerents.[63] For example, as World War I began in August 1914, the British cableship Telconia cut Germany's undersea cables, and reeled in the loose ends to prevent repair.[64] Governments have conducted radio jamming in both peace and war for over 60 years, beginning with Austria's efforts to block propaganda broadcast from Nazi Germany in 1934.[65] Finally, ruses have been part of warfare for millennia and their legitimacy has been explicitly recognized;[66] just as the original, ancient Trojan Horse was legal, so too might be some "Trojan Horse" pieces of software.

Major Limitations on Information Warfare

Despite the novelty of some information warfare techniques, international law poses some constraints on the conduct of information warfare, just as it does on the traditional forms of warfare that use kinetic force for their impact. Nevertheless, characteristics of information technology and warfare pose problems to those who would use international law to limit information warfare, and leave legal space for those who would wage such warfare.

Neutrality and National Sovereignty

By treaty as well as by longstanding customary law, the territory of neutral states is supposed to be inviolable by the forces of belligerents.[67] Apparently, then, an attack

through a network that crosses neutral territory, or using a neutral country's satellites, computers, or networks, would infringe upon that neutral's territory, just as would an overflight by a squadron of bombers or an incursion by armed troops. The attack would thus be considered illegal and, perhaps, an act of war against the neutral.[68] Conversely, a neutral's failure to resist the use of its networks for attacks against another country may make it a legitimate target for reprisals by the country that is the ultimate target of the attacks.

Although the argument that electronic incursion would violate neutrality is strong, a counter-argument exists. The encroachments beyond a nation's borders that may violate its neutrality have, in the past, been physical intrusions by troops, ships, or planes. Attacking a neutral's networks, satellites, or computers might not violate the state's neutrality because it might involve no physical encroachment (and might not even constitute an "attack" in the first place[69]). Significantly, although neutrals must not allow any belligerent to move troops or supplies through their territory,[70] or to erect military radio stations there,[71] neutrals have no such obligation to prevent belligerents from using their publicly accessible communications equipment.[72]

Further, as a practical matter, despite an unambiguous rule to the contrary,[73] belligerents have quite significantly violated prohibitions against the erection and use of non-public military communications facilities in neutral territory for military purposes. Thus, the vitality of rules regarding neutrals and telecommunications may have been weakened, as countries have acted as if those laws did not, in fact, have legal force. During World War II, for example, belligerents on both sides took advantage of the neutrality of Portugal, as well as perhaps Turkey and Switzerland, by constructing and using telecommunications facilities for military purposes within those states.[74] In sum, it is not obvious whether the use of a neutral nation's computers, networks, and communications facilities would violate that nation's neutrality, or open that nation up to belligerent reprisals.

International Humanitarian Law

International humanitarian law would seem to welcome the nonlethal "combat" that information warfare promises, but that body of law, which is a combination of conventions and longstanding customary law,[75] may constrain information warfare activities as it does traditional warfare. The fundamental principle of this body of law is that the permissible methods of hurting an enemy are not unlimited,[76] and that the cruelty of war must be mitigated and circumscribed.[77] Nevertheless, although that principle unquestionably survives, even if it is sometimes honored only in the breach, it is not obvious that all types of damage that information attacks would inflict are the kinds of injuries against which humanitarian law endeavors to protect.

Although humanitarian law protects combatants as well as noncombatants, the most significant relevant general tenet of humanitarian law is the protection of civilians. This principle was codified over a century ago in the St. Petersburg Declaration of 1868, which recognized that the only legitimate object of war was to weaken an enemy's military forces.[78] Civilians, as such, may not be the object of an attack. Much of the law addressing the fate of civilians stems from concern over artillery bombardment, and later aerial bombing, as that was how civilians, unless they were loitering near a battlefield,

were most likely to come under fire, and it consistently places civilians off limits for attack. Under the Hague Convention (IV) of 1907, military forces could not attack or bombard "by whatever means" undefended towns, dwellings or buildings,[79] a provision that has carried over into the charter of the tribunal considering war crimes in the former Yugoslavia.[80] Similarly, the Charter of the Nuremberg Tribunal condemned wanton bombing of civilian targets.[81]

Despite such legal protections, the reality is that civilians are often victims of modern warfare, without legal consequences for those who hurt them. Nevertheless, when attacks are planned and executed, attackers are supposed to try to avoid injuring civilians, even collaterally. Attacks are to be directed solely toward "military objectives," which have been defined (to the extent such a definition is meaningful) as "those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[82] To the end of confining attacks to military objectives and limiting civilian casualties, nations may not use weapons that make it impossible for their targeters to distinguish between civilian and military targets (and of course, the targeters must make such distinctions).[83]

The planning and execution of attacks must also include considerations of "proportionality" between civilian damage and the military objective attained. Proportionality is a dual doctrine, arising from customary international law. It applies to both whether a given level of force is appropriate in response to a particular grievance (as part of the law of the use of force, or jus ad bellum),[84] and whether a given action is appropriate in light of its objectives and the casualties that will result (as part of the law of armed conflict, or jus in bello).[85] In the context of humanitarian concern, proportionality derives in part from the Christian "just war" doctrine. Commanders must minimize civilian casualties, subject to the need to accomplish a particular military mission, and they must weigh the cost of civilian lives against the benefit to be gained by the mission.[86]

On its face, international humanitarian law anticipates technological change relatively well. Even though some information warfare weapons and techniques could not even have been contemplated when the humanitarian legal principles were developed, those principles can still apply. The "Martens Clause," which has been a part of major humanitarian conventions since 1899, asserts that even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and from the dictates of public conscience, and that they are not left to the arbitrary judgment of military commanders.[87] In other words, for purposes of humanitarian law, attacks will be judged largely by their effects, rather than by their methods.

Despite its apparent flexibility in coping with technological change, international law may not easily deal with information warfare. It seems obvious that information warfare attacks that were the direct and intentional cause of noncombatant death and destruction-such as disruption of an air traffic control system that caused a civilian airliner to crash,

or corruption of a medical database, causing civilians or wounded soldiers to receive transfusions of the incorrect blood type-could violate the laws of war.[88] It is less obvious that attacks with less tangible results, such as the disruption of a financial or social security system, or the disclosure of confidential personal information, constitute the sort of injury against which humanitarian law is supposed to protect civilians, even though for some victims, the consequences of disruption of, say, the banking system, could be more painful than a bombing that damaged a dwelling.

In considering whether information attacks against civilians may violate humanitarian law, it is important to remember that all wars cause suffering for civilians, ranging from deprivations as resources must be diverted to military purposes, to disruption of government services, to destruction of buildings and loss of life, to outright mass starvation, without apparent legal consequences, and often with the law's blessing. Indeed, although the legality of such a strategy might now be questioned,[89] the starvation of the Japanese population was part of the U.S. naval strategy in World War II. Similarly, the hardship imposed on Iraqi civilians by the U.S. and UN embargo against Iraq was supposed to either influence Saddam Hussein or convince the Iraqi people to overthrow him.

The dual-use nature of many telecommunications networks and much equipment further complicates the questions of the applicability of humanitarian law as a constraint on information warfare. These dual uses contribute to the blurring of the distinction between military and civilian systems and, consequently, between military targets, which are legitimate, and civilian ones, which are not. Some information weapons may thus not permit their users to distinguish between military and civilian targets. In the United States, for example, it has been estimated that 95% of the telecommunications of the Department of Defense travel through the Public Switched Network,[90] and during the Persian Gulf War, commercial communications satellites reportedly carried almost a quarter of the U.S. Central Command's transcontinental telecommunications.[91] Additionally, U.S. military forces are particularly dependent upon non-military systems for deployment and logistics.[92] Attacks with military objectives might thus necessarily be directed at predominantly civilian systems, with corresponding injury to the civilians who depend upon them.[93] As Vice Admiral Arthur Cebrowski stated in 1995, "There is no logical distinction...between military or civil systems or technologies. [Therefore] there is also no technical distinction between exploitation, attack or defense of the information warfare target set."[94]

The interdependence and interconnectivity of civilian and military systems may further exacerbate the difficulty in distinguishing among civilian and military targets. Attacks directed at predominantly military targets may cause civilian systems that are connected to those military systems to fail; alternatively, a virus that is directed toward an adversary's military systems may spread, inadvertently or otherwise, into civilian (and even friendly) systems. Furthermore, attacks on systems that would otherwise be legitimate targets may be impermissible because of the danger to civilians that system malfunctions might cause. For example, an attack on a military power facility might pose problems if that facility's failure could release dangerous materials into the atmosphere.[95]

Manipulating Enemy Perceptions

Spurring Internal Turmoil. Techniques such as video morphing and communications spoofing may make it possible for a country to manipulate the perceptions of its adversary's leaders and populace. The country may spread confusion or disaffection by covertly altering official announcements or news broadcasts, or it may confuse or frighten leaders by spoofing intelligence or other government communications. In principle, these actions would not violate the laws of war.

Taken to the extreme, however, manipulation of news or intelligence in certain cases might be considered the proximate cause of genocide or other atrocities. As Colonel Richard Szafranski has suggested, manipulating an adversary nation to the extent that its citizens or leaders become unhinged from reality, especially when the effects cannot be known or controlled, may be no less wrongful than to force another nation into starvation or cannibalism.[96] The potentially dangerous results of perception manipulation are more than theoretical. Some observers believe that "hate radio" contributed to, or even sparked, genocide in Rwanda and the former Yugoslavia. The use of propaganda, "video morphing," or deceptive broadcasts to the extent that they spur unrestrained civil war, or even genocide, may thus be illegal.[97]

Perfidy. Although ruses are unquestionably permissible in war, not all acts of deception are. Certain acts of treachery or "perfidy" are forbidden by longstanding customary law and by several conventions. While ruses (such as the threatened U.S. Marine landing in Kuwait during the Persian Gulf War) are acts planned to mislead an enemy, as by causing him to become reckless or choose a particular course of action, perfidious acts are designed to convince the enemy that the actor is entitled to protected status under the law of war, with the intent of betraying that confidence.[98] Perfidious acts include feigning a truce or surrender, injury or incapacitation, civilian status, or other protected status, such as that of UN or neutral forces, for purposes of attacking the enemy.[99] Similarly, attacking while wearing the enemy's uniform is prohibited.[100]

Information warfare attacks that involve distorting enemy perceptions may be limited by prohibitions against perfidy. For example, manipulating enemy visual, sensing, or other information systems so that enemy forces wrongly believe that U.S. troops are surrendering would certainly seem perfidious, as would causing them to believe that U.S. combat vehicles were medical vehicles or those of neutrals. Similarly, manipulating an enemy's targeting database so that it believed that a U.S. division headquarters was a hospital would be wrong.[101] Less obviously, manipulating identification signals so that a nation's forces believe that the enemy personnel or vehicles that are approaching are actually friendly forces would arguably come under the norm underlying the prohibition against attacking while wearing enemy uniforms. On the other hand, because of the longstanding view that communications may be disrupted, and because, unlike uniforms, information systems are in no way required by the laws of war but are rather combat aids, such tactics might seem less treacherous than would taking advantage of the requirement that troops wear distinct uniforms to set themselves off from their foes and civilians.

"Peacetime" Use of Information Warfare and Problems of Definition

Is Information Warfare "Warfare"?

Definitions and Prohibitions. A side-effect of technological change is that the new activities that it enables may not fit within established legal categories. For example, aerial surveillance has historically been restricted by the sovereignty of each state over its airspace. The development of satellite and space technology in the 1950s later enabled surveillance from orbit. Although such orbital surveillance was functionally the same as aerial surveillance, international law has chosen to consider it as a distinct activity, subject to the universal freedom of actions in space. This characterization was not obvious or required by contemporary understandings of international law; more likely, most countries who wanted to apply traditional understandings of sovereignty to orbital surveillance, such as several African states, lacked the capacity to do anything about it.[102] A fundamental threshold question that arises from the development of information warfare techniques is thus the definitional one. Has the development of information warfare technology and techniques taken information warfare out of the existing legal definition of war? Simply, it is not obvious that all information warfare attacks, including some that would inflict serious hardship upon their targets, are what has previously been included within our understanding of "war."[103] Similarly, the "damage" that such attacks would inflict, particularly upon civilians, may not be the sort of hardship that the historical and conventional laws of war were intended to alleviate. Consequently, there may be confusion over what limits may apply to the conduct of information warfare, and when information warfare attacks may be carried out.

War, as we have traditionally understood it, inherently includes armed forces, force, and violence.[104] The efforts of the United Nations to pursue a more peaceful world are instructive on this point. Article 2(4) of the UN Charter, for example, forbids the threat or use of force against the territorial integrity or political independence of another state. This prohibition has been applied only to physical force since the drafting of the Charter. Most relevantly, the United States and its allies have understood the provision as not applying to economic coercion, although many questioned that view during the 1973 Arab oil embargo.[105] Further, during the drafting of the Charter, when Brazil proposed including "economic measures" with "force," the proposal was rejected by a vote of 26-2.[106] Consistently, Article 51 of the Charter recognizes a state's right to use force in self-defense against an "armed attack."[107]

Although lacking some of the formal legal authority of the Charter, the United Nations General Assembly's declaration defining "aggression" also reveals explicit contemplation of armed forces or military might.[108] The declaration defines aggression, which the Security Council is empowered to address,[109] as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[110] The first use of armed force by a state would constitute prima facie evidence of aggression.[111] The declaration sets out the following as a non-inclusive list of those acts that would qualify as aggression:

- The invasion or attack by the armed forces of a state of the territory of another state, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of all or some of another state's territory.

- Bombardment by the armed forces of a state against the territory of another state or the use of any weapons by a state against the territory of another state.[112]

- The blockade of the ports or coasts of a state by the armed forces of another state.

- An attack by the armed forces of a state on the land, sea, or air forces, or marine and air fleets of another state.

- The use of armed forces of one state which are within the territory of another state with the agreement of the receiving state, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement.

- The action of a state in allowing its territory, which it has placed at the disposal of another state, to be used by that other state for perpetrating an act of aggression against a third state.

- The sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another state of such gravity as to amount to the acts listed above, or its substantial involvement therein.[113]

Other legislative practice of the United Nations reinforces the view that "aggression" is limited to the use of force. In 1953 Iran pressed the United Nations for an understanding that any act serving the same ultimate purposes as an armed attack or involving coercion to endanger independence was "aggression," but the United Nations has never adopted that view.[114]

Further affirming the kinetic view of war is the definition of "attacks" as enunciated in the 1977 Additional Protocol to the Geneva Convention. That document, which the United States has signed but not ratified, embodies much customary international law.[115] It defines "attacks" as "acts of violence against the adversary, whether in offense of defense."[116] Additionally, the issue of whether an information warfare attack constitutes "armed attack" for purposes of self-defense under the UN Charter is discussed in Part III.

Some forms of attack under the information warfare rubric fit comfortably within the above definitions of war, force, aggression, and attack. For example, the use of precision-guided munitions against a military communications post could certainly constitute war. Although the disruption of a social security system database through the use of a virus or hacking during hostilities could certainly be part of a war, it is less obvious that such attacks would by themselves constitute acts of war, because of their nonlethal, nondestructive (in a direct, physical sense), non-physically intrusive character.

On the other hand, it is certain that a state of "war" can exist in the absence of what we have traditionally understood as fighting. Wars do not always end simultaneously with the cessation of combat; rather they generally may require some sort of closure, both for international and domestic legal purposes.[117] For example, the United States did not give up its status as a belligerent in World War I until 1921, even though fighting ceased in 1918;[118] World War II did not end for several countries until well after 1945; and Israel and its Arab foes have endured years of largely combatless war. Conversely, although formal declarations of war are virtually nonexistent in the modern era, nations could certainly declare war on each other without actually engaging in battle.

Where the applicability of a principle of law is not immediately ascertainable, it is often helpful to examine the intent underlying that legal principle or statute. Unfortunately, that intent is insufficiently instructive.

The fundamental document of the modern international legal system is the Charter of the United Nations, which was signed in San Francisco in 1945. According to the Charter's Preamble, the aim of the United Nations' founders was, in relevant part, "to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind."[119] To pursue those ends, the founders resolved to:

- practice tolerance and live together in peace with one another as good neighbors, and
- unite our strength to maintain international peace and security, and
- ensure by the acceptance of principles and the institution of methods, that armed force shall not be used save in the common interest, and
- employ international machinery for the promotion of the economic and social advancement of all peoples.[120]

The stated purposes of the United Nations are:

1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;[121]
2. To develop friendly relations among nations based on respect for the principle of equal rights and self determination of peoples; [122] and
3. To achieve international cooperation in solving international problems of an economic, social, cultural or humanitarian character.[123]

Members of the United Nations, and the organization itself, are pledged to act in accordance with the following relevant principles:

> All members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered;[124] and
>
> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[125]

The UN General Assembly has set out its interpretations of nations' obligations under the Charter. The Declaration of Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations opposes all forms of coercion, including economic pressure against a state "to obtain from it the subordination of the exercise of its sovereign rights."[126] In a similar vein, the General Assembly also set out a Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States, which included similar language against the subordination of sovereign rights, and asserted:

> No State has the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned;[127]

The problem in using the fundamental principles laid out in these declarations as tools in interpreting whether the prohibitions on the use of armed force would apply to certain forms of information warfare is that to do so would be to rely upon reasoning that is either circular or demonstrably unrealistic. For example, the UN Charter language about the "scourge of war," "threats to the peace," "respect for...international law," preventing the use of "armed force," settlement of international disputes through "peaceful means," and refraining "from the threat or use of force" is only relevant to nonlethal information warfare attacks if we have already established that the information warfare attacks are, indeed, "war," "force," "unpeaceful means," or whatever other term would apply to something we would be trying to forbid. Similarly, the Friendly Relations declaration's prohibition of the use of coercion to force the subordination of the exercise of a state's "sovereign rights" applies only to the extent that we have determined that the information warfare attack violates those sovereign rights, which are nowhere defined. To read the provision otherwise would be to forbid diplomacy or other forms of inducements.[128]

Finally, the declaration on intervention does not really define intervention, and in any event, does not equate nonmilitary intervention with aggression or the use of force, thus leaving room for attackers to defend their conduct. Indisputably, although virtually all states purport to recognize the norm of nonintervention, intervention of various kinds occurs frequently, without constituting aggression or war. The declaration thus leaves us with no principled way to place information attacks along a continuum of intervention stretching from a nation's leader publicly meeting with one candidate in a neighboring

country's election, to funding of foreign political parties, to bribing government officials, to arming dissidents, to bombing military or police installations.[129]

Reliance upon exhortations to cooperative or friendly behavior as aids in interpreting the applicability of the prohibitions on the use of force to information warfare would also require circular reasoning and disregard actual state practice, which is itself a source of international law.[130] None of these documents mandates a unified, consistently harmonious world. Because the United Nations was established to promote the peaceful resolution of conflict, it implicitly assumes that conflict will arise, and that nations will use various means to resolve them. Information warfare techniques are thus inappropriate to resolve conflicts only if it is determined that they are not peaceful means, the very determination the provisions should help us to make.

The Ability of States to Hurt Each Other. It is important to remember that merely because a government action weakens another country's military forces or hurts its people, does not make that action an act of war, aggression, or force. Longstanding international practice recognizes that nations may inflict great hardship upon each other and their respective citizenries without such infliction constituting the use of force or a violation of international law. In the absence of any international agreement, nations have no underlying legal obligation to deal with each other.[131] A government may thus legally withhold a resource, such as fuel, food, or even medicine, without which the population of another nation might suffer severely. A country may even pressure others not to deal with a third country.[132]

Economic boycotts, embargoes, and other sanctions have been common tools of international coercion in the twentieth century, especially after World War II. Countries of virtually all political persuasions have tried to use the infliction of hardship as a way to convince governments to amend policies.[133] For example, in 1908 the Ottoman Empire boycotted all goods from Austria-Hungary in response to that nation's annexation of Bosnia and Herzegovina.[134] In 1948, the Council for Mutual Economic Assistance (COMECON) imposed a boycott on trade with Yugoslavia after the rift between Marshals Stalin and Tito.[135] The United States and United Kingdom organized an international boycott of Iranian oil after the short-lived government of Mohammed Mossedegh nationalized Iran's oil industry in 1951.[136] Finally, in the decades following the 1948 Arab-Israeli war, the Arab League instituted primary, secondary, and tertiary boycotts against Israel, against companies that did business with Israel, and against companies that did business with companies that did business with Israel.[137]

Similarly, where it has not internationalized a canal, the country through which a canal travels may close that waterway to other nations, even when doing so would hurt those who depend upon the shipping that must travel through it.[138] Furthermore, states have routinely practiced "dirty tricks" against each other, ranging from economic espionage to sabotage of exports and imports and beyond, with few, if any international legal repercussions.[139]

The Significance of Armed Force. Comparison of information warfare attacks and naval blockades may be instructive for understanding the possible place of information warfare

under international law. As discussed above, it is not obvious whether nonlethal attacks that are neither physically intrusive nor physically destructive would constitute acts of "war," "force," or "aggression." Naval blockades, in contrast, are recognized as forceful and potentially aggressive acts, even though some effective blockades may be nonviolent, as ships either avoid the blockaded ports or are diverted peacefully.

The effects of naval blockades and information warfare attacks can be similar. Naval blockades prevent the transport of people and products into the target country or area, and may paralyze an economy. In the past, where intercontinental communication was largely by ship, a blockade would keep out information as well. An information warfare attack may also make transport of people and products impossible, paralyzing an economy, and it too may block the spread of information (especially as in an "infoblockade").

The primary distinctions then between a naval blockade and some information attacks might be that the blockade is executed by military forces and includes the threat (or actual use) of physical military force, while the information warfare attack may be executed by military or civilian personnel and contains no physical component or threat. The relevance of these distinctions will be significant for the treatment of information warfare under international law.

In sum, international law seems to draw a strong distinction between traditional, kinetic force and the infliction of hardship or suffering on a government or population. Without getting overly philosophical about the meaning of "violence," the experience of the United Nations and United States in Iraq is instructive. The United Nations has enforced an embargo against Iraq since 1990, with reportedly devastating effects on the Iraqi population and economy. During that time period, the armed forces of UN members, mostly the United States, have taken military action on several occasions, but only in response to specific perceived Iraqi provocations, such as the planned assassination of former U.S. President George Bush or the launching of missiles at U.S. planes enforcing a no-fly zone. If this distinction between the use of physical force and the infliction of hardship is legally valid, nonviolent information attacks may not be considered to be "war," and thus might not be subject to the legal constraints that govern warfare.

The Importance of Categorization

The issue of how to categorize information warfare attacks is of more than academic interest. First, whether or not an information warfare attack can be considered an act of "war," "force," or "aggression" is relevant to whether a forceful response can be justified as self-defense, as well as to the issue of whether a particular response would be proportionate to the original attack.[140] Conversely, whether an information warfare attack can be considered the use of force goes to the attack's legality as a coercive measure in "peacetime." If a computer or communications intrusion or manipulation is considered the use of force (as in, say, a naval blockade or the bombing of a radar facility), then it could be an illegitimate tool of international coercion. But if it is the rough equivalent of, say, trade sanctions, then it might be appropriate in a peaceful context. Additionally, characterization of an action as "war" would affect the rights and responsibilities of nations that are neutral in the ongoing conflict.

Finally, characterization of attacks and the damage they cause is relevant to the status of those attacks under international humanitarian law, specifically those provisions that protect noncombatants from attacks and the consequences thereof. First, if an information warfare attack is not considered to be an act of "war," then humanitarian law may not apply; the attack could be considered to be equivalent to such measures as closing a canal, or refusing to trade, the sort of act that nations appear to have the legal right to commit. Second, as discussed earlier, it is not settled that the non-physical or indirect damage that some information warfare attacks could cause are the sort of effects against which humanitarian law protects noncombatants. If humanitarian law does not apply, then countries may legally pursue information warfare without (legal) concern for the harm that civilians might suffer.

Difficulty in characterizing certain forms of information warfare as "force," "war," or "aggression" under international law does not mean that international legal institutions cannot respond to such attacks, though. For example, Chapter VII of the UN Charter gives the UN Security Council the authority and responsibility to determine the existence of any "threat to the peace" or acts of aggression,[141] and the Council can recommend and lead responses thereto.[142] Many information attacks that may not constitute "force" or "aggression" could certainly be considered threats to the peace and thus subject to Security Council action, perhaps including the use of military force. After all, anything that would anger a government to the point that it might feel the need to resort to military action could thus "threaten" the peace, even if the provocative action was not technically illegal. Nevertheless, because any Security Council action would be subject to international political negotiation and maneuvering, as well as a veto by one of the permanent members of the Council, such a response would likely not be quick, sure, or a significant deterrent to a state or non-state entity that was considering an attack, nor might it provide solace to the attack's target.

Chapter 3: Responding to Information Warfare Attacks: International Legal Issues and Approaches

Attacks Against Information Systems: Methods and Motives

Although the United States is believed to lead the world in information warfare capability, other countries are pursuing such capabilities, as perhaps are transnational criminal organizations or terrorist groups. Because of the perceived overwhelming traditional military might of the United States and its allies, and because international networks may offer a way for adversaries to strike at the U.S. homeland without needing the sort of logistical and military capabilities that a traditional attack would require, it seems likely that the United States or one of its technologically and economically developed allies will suffer some sorts of serious information warfare attacks. If such an attack comes, the United States (or any other victim) may find its response hindered, as it may find both that the norms arising from traditional concepts of the international system of sovereign states may conflict with the physical reality of the newly wired world, and that the international legal system may not yet have arrived at rules applicable to such attacks. The United States may thus face difficulty in tracing an attack across national boundaries, gaining authority over the attackers, and determining the appropriate responses the attack.

Other observers have laid out in detail the types of information warfare attacks that adversaries may conduct against U.S. security facilities, the U.S. homeland or infrastructures, or the facilities of other countries.[143] These adversaries may include foreign governments, including those of some "friendly" countries; state-supported or independent terrorist organizations, which may be international in composition or aim; transnational criminal organizations, such as the Russian mafiya or Latin American drug cartels; foreign competitors of U.S. companies; domestic terrorists or other criminals; or "hackers," who conduct mischief of varying severity using computers, telephones, and networks.

Such attacks may be part of armed conflict or a prelude to war. They may constitute a warning or threat to influence a government's decision makers as they contemplate particular courses of action. They may be part of an economic conflict, either between nations or between corporations (and in many countries, such a distinction is blurred). They may be terrorism, or part of other efforts to attract attention to a cause.[144] They may be part of crime, as a mechanism of theft of funds or valuable data, as part of extortion, or as part of an effort to hinder law enforcement. Finally, the attacks may be motivated by perversity, as individuals or groups attack systems because they can, or to show off, or because of various personal shortcomings.[145]

Identification Of An Attack

The first dilemma that a country that has suffered an information attack may face in responding to the attack may be to identify an event as an actual attack. Especially when an attack does not come during a period of heightened international tensions, it may be

difficult for investigators to distinguish a catastrophe resulting from a "natural" or "accidental" computer error from one stemming from malice.

Physical attacks should be distinguishable from accidents or malfunctions, as the culprits must come into some proximity with their target, and they may leave some physical evidence behind. As Aristide Briand said, "A cannon shot is a cannon shot; you can hear it and it often leaves traces."[146] But even so, the causes of catastrophes may be hard to ascertain, especially when they involve complex systems that may not be fully understood. For example, despite exhaustive investigations, the separate but similar crashes of two Boeing 737 passenger jets remain unexplained.[147] Furthermore, and most dramatically, the mystery of the July 1996 crash of TWA Flight 800 into Long Island Sound, which some immediately assumed was a terrorist incident, remains unsolved, and investigators did not publicly rule out the possibility of sabotage until May 1997.

Computer-based attacks may be even harder to distinguish from innocent malfunctions. If the attack is carried out across a network, the culprits may never be physically close to the target (perhaps never entering the same continent), and they may leave no tangible evidence. Attacks or sabotage using viruses, logic bombs, or simply buggy software may be particularly difficult to detect quickly, if at all, because of the complexity of systems and the frequency of unintentional errors in publicly shipped products.[148]

Software errors or conflicts are known or suspected to have caused a number of incidents that might have seemed to be intentional attacks on important systems, products, or weapons by criminals, terrorists, or even enemy nations. Perhaps the most dramatic example occurred on Martin Luther King Day in 1990, when the AT&T long distance network failed for nine hours. Although the actual source of the failure was ultimately attributed to a faulty software update, many believed that hackers had actually caused the system to crash.[149] Perhaps more frighteningly, a software error caused a Canadian nuclear reactor to release thousands of liters of radioactive water in 1990.[150] Similarly, a timing delay in targeting software caused a British Royal Air Force pilot to drop a practice bomb on a British aircraft carrier in 1992,[151] and it has been suggested that the crashes of two U.S. Air Force F-117 fighters in identical, suspicious circumstances were due to a bug in their software.[152] Systems may even be inadvertently sabotaged by their creators. For example, in October of 1994, Adobe Systems, Inc. accidentally shipped a "time bomb" in a version of its popular Photoshop software program. The time bomb, which was to cause the program to stop running after a particular date, had been inserted into the code to force those using a pre-release version of the program to upgrade to the final shipping version, only when it was time to ship the product, nobody remembered to take it out.[153]

An incident during a time of heightened international tensions might seem to present evidence that wrongdoing is afoot. Nevertheless, such evidence might not be compelling alone, as times of stress are also the times when complex, brittle systems may be most likely to break down.[154]

The difficulty in distinguishing attacks from accidents is particularly significant in light of the apparent U.S. preference for acting under the auspices of international coalitions.

Unless the United States is prepared to act alone, the evidence it uncovers that an incident was the result of an attack, and that the attack stemmed from a specific source, must be sufficient not only to convince U.S. policymakers, but also to convince foreign governments. There is no set standard of proof for U.S. officials to meet; the deliberations of the UN Security Council, and those of foreign governments, are political rather than judicial. Diplomacy, including carrots and sticks, may be more significant than persuasive, logical arguments. That foreign governments may be skeptical of both U.S. intentions and U.S. technical methods of detection complicates the tasks of investigators and policymakers alike.

After extensive investigation of the explosion of Pan Am Flight 103 over Lockerbie, Scotland, in December 1988, for example, the United States and United Kingdom tried to convince the Libyan government of Muammar Qadhafi to extradite the Libyan agents who were allegedly responsible for the bombing. In their efforts to obtain UN sanctions against Libya for its refusal to extradite the suspects, they presented evidence to the other members of the UN Security Council, which held meetings in camera, with no public minutes taken, to protect the confidentiality of the evidence and the Council's deliberations.[155] Qadhafi refused to extradite the suspects and demanded that the United States provide him with evidence to support its charges, which he mocked.[156] Perhaps to protect intelligence sources and methods, the United States refused to provide Libya with the evidence.[157] Despite ongoing sanctions, Qadhafi has neither acknowledged the value of the U.S. evidence nor complied with the Security Council's demands.

Investigation of Network Attacks and The Problem of Territorial Jurisdiction

Investigators tracing attacks across computer networks may be stymied by a collision between fundamental principles of physics and those of international law, namely that electrons may flow through networks freely across international borders, but the authority of agents of national governments does not. Simply, an attack may come from a foreign country, or may be routed through computers in several countries, but law enforcement or national security personnel cannot unilaterally launch pursuit into networks in other countries. Under the principle of sovereignty each government has exclusive authority over events within its borders.[158] Investigators will thus need foreign cooperation or help in their investigations or, with proper domestic authorization, they will need to operate covertly.

Historically, foreign agents have not been permitted to operate physically on a state's territory without that state's permission.[159] As the International Court of Justice held in the 1949 Corfu Channel case, when Great Britain wanted to investigate and stop the Albanian mining of the channel, intervention in another state to secure evidence is prohibited.[160]

Although the principles of sovereignty were conceived when international law contemplated only physical intrusions into a nation's borders, national governments would probably try to apply the principles to intrusions into computers, networks, or data banks, and they would probably succeed. Individual governments have already exerted

authority over information in domestic systems just as they would if it had physical form; many European governments, as well as the European Union, for example, have enacted data protection codes that forbid the transport or transmission of certain personal data to countries (such as the United States, perhaps) that do not provide sufficient protection for that data.[161] Governments may thus go so far as to consider the act of investigation by foreigners of criminal misuse of their systems to be a form of computer crime, or worse.[162]

The 1994 intrusion into the computers at the U.S. Air Force's Rome Laboratory in New York hinted at the problem of the collision between sovereignty and a wired world. That spring, two hackers, both now believed to have been British, broke into and took control of the operational network at the U.S. Air Force's command and control research facility at the Rome Labs. Air Force investigators were observing one attacker in the Rome computer when he accessed a system at the [South] Korean Atomic Research Institute, obtained all of its stored data, and deposited that data into the Rome Labs system. The investigators, initially fearing that the system belonged to North Korea, were concerned that the North Korean government would interpret the intrusion and transfer of data to the U.S. Air Force system as an act of war, at a time of sensitive negotiations with North Korea over its nuclear weapons program.[163]

Although the stronger view is probably that government agents' intrusion into a foreign computer would constitute a violation of the target nation's sovereignty, it is important to note that not all electronic crossing of boundaries is considered that way. For example, orbital remote sensing, including the bouncing of such signals as radar off a country's territory, is now so universally accepted that it is conducted by private entities, which may sell the products of their sensing on the open market.

Furthermore, particularly where they do not interfere with registered stations, countries have no obligation to keep their radio broadcasts from penetrating others' borders.[164] Weak authority even supports the proposition that the target country may not resist such broadcasts by jamming.[165] Even if the dubious international legality of unauthorized cross-border electronic intrusion by a government's agents were to become accepted, those intrusions could still violate the target country's domestic laws, if any, on espionage or computer intrusion. Just as it would be hard for U.S. authorities to exert authority over foreign computer attackers, though, foreign governments would face difficulty in enforcing their laws against U.S. agents operating from computer terminals within the United States.

The conflict between international networks and national sovereignty is not merely an academic one. The U.S. Government has already had to face the problem of pursuing foreigners who have broken into U.S. computer systems from abroad for malicious purposes, although these attackers have apparently not succeeded in causing, or have not attempted to cause, significant destruction or denial of service. Attackers have complicated U.S. investigatory efforts by "looping and weaving" their attacks through several foreign countries so that investigators cannot follow the trail. For example, to stymie tracing efforts, the attackers who invaded the Rome Labs computers wove their

way through phone switches in Columbia and Chile before entering Rome Labs through commercial sites in the United States.[166]

The apparent widespread, inexpensive availability of the technology necessary for international attacks across computer networks, combined with the anonymity that the technology may provide its users, may complicate the efforts of investigators to determine whether responsibility for an attack carried out by an individual or group rests with a foreign government, and would certainly make it more difficult to convince other nations or international organizations of that government's role. This availability could reduce the need for terrorists or similar actors to seek state support. It should also give states that do support terrorism claims of "plausible deniability" that are stronger than those of states that have supported terrorism in the past. Conversely, the inexpensive, small, and ubiquitous technology may make it harder for states to live up to their obligation to prevent their territories from being used for attacks against other states. As Paul A. Strassmann, former Director of Defense Information and Principal Deputy Assistant Secretary of Defense for Command, Control, Communications and Intelligence, has stated, "Info-assassin paraphernalia is booming, and it's gory stuff you can buy....There is also a wide range of people available for hire to carry things out, many of them ex-intelligence agency people."[167]

The tasks of investigators, policymakers, and diplomats are made harder by the uncertainty that arises from the ability of users (or abusers) of computer networks to hide their identities through such techniques as "spoofing" so that others may be blamed for their misdeeds. In fact, absent a credible admission of responsibility, it may be impossible to attribute an attack to its actual source with any degree of confidence. This uncertainty may have ramifications both for national security and for law enforcement.[168]

Cooperation

Further complicating nations' attempts to trace attacks against them is the international investigatory legal regime, or lack thereof. First, in the absence of a treaty, countries have no underlying obligation to cooperate with each other in their law enforcement or national security investigations. The mere fact of noncooperation probably cannot be considered evidence of implication in the attack. Even where they had no involvement in, or sympathy for, an attack, hostile or indifferent nations may be unwilling to assist foreign investigators, whom they may view as spies. Even largely friendly governments may be reluctant to cooperate, often for domestic political reasons.

International law enforcement agreements may not be adequate to support an investigation. For example, treaties of mutual legal assistance, which may institutionalize cooperation between countries' law enforcement agencies, generally contain exceptions that permit parties to refuse cooperation under certain circumstances, such as to protect "sovereignty, security, or similar essential interests."[169] In the context of computers, networks, and databases that may implicate a country's national security interests, its technological development, security of its financial and communications infrastructure, or the privacy of its citizens, and where governments may not feel confident about their

ability to monitor foreign (especially U.S.) investigators' activities, some nations may likely at least consider taking advantage of any loopholes they can.

Even where other countries are cooperative, mechanisms of international cooperation, such as letters rogatory,[170] may be prohibitively slow, particularly given the speed of communications and action across networks. Furthermore, and perhaps most significantly, requesting cooperation, even through such an organization as Interpol,[171] would require the substantial involvement of foreign governments' officials and could expose them to information about the victim's intelligence capabilities or the vulnerabilities of the systems and networks they depend upon.

Given the difficulties of international cooperation discussed above, some in the U.S. Government may advocate that it unilaterally pursue its investigation without the cooperation of countries whose computers or networks have been used for attacks against U.S. systems. Although such a course of action seems likely to violate the sovereignty of those nations, and may be inconsistent with U.S. responsibilities under individual treaties of legal assistance, it would not in itself violate international law any further. The investigation would probably be characterized as "espionage," which does not violate international law, although it violates the domestic law of virtually all states. The U.S. Government would need to consider the diplomatic, political, and precedential ramifications that would arise if such an investigation were detected, just as it would have to in the case of more traditional forms of espionage or covert action.

Responding

Extradition

Obviously, a government cannot respond to an attack successfully unless it can identify the attack's source.[172] If the culprits can be identified, the options available for the victim state are unsettled and potentially unsatisfactory. As discussed above, it may be difficult, if not impossible, to tie the individual culprits to state support. A victim state may therefore need to proceed as if a given attack were a purely criminal matter, and request that the state in which the culprits are present extradite them to its territory for trial. Even where the victim has substantial grounds for believing that state support existed, it may proceed with the extradition request, because denial of the request may be seen in world forums, as well as in its domestic politics, as further evidence of that state's complicity. The UN sanctions against Libya in the wake of the Lockerbie bombing, for example, stemmed not as directly from Libya's involvement in the bombing, as they did from Libya's refusal to extradite the alleged bombers to the United States or United Kingdom, in violation of Security Council Resolution 748. The significance of political considerations in such a calculus is emphasized by the fact that at the time the sanctions were promulgated, Libya, which had claimed to be willing to try the alleged culprits, had not actually violated the procedural terms of the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation, which permits a signatory to extradite or try a suspect (although, of course, bombing a plane would, indeed, violate the convention).[173]

The ability of a victim state to gain custody of those who have attacked its systems from abroad is complicated by the collision of the longstanding international state system, the

international nature of networks, and the relative historical novelty of computers and networks. For a country to apprehend an alleged criminal in a foreign country and transport the culprit to the requesting country for trial, certain conditions must exist. First, an extradition treaty must bind both countries, as there is no underlying right of extradition under international law.[174] Extradition treaties may be bilateral or multilateral, and they may apply to a broad range or to discrete categories of offenses.[175]

Second, the requesting country must have jurisdiction to prescribe the activity for which it seeks extradition; in other words, it must be within the power of the state to apply its laws to the relevant conduct. States base their claims to jurisdiction over criminal suspects on five general theories: first, and most simply, the territorial theory, by which states claim jurisdiction over those who act within their territories; second, nationality, by which states claim jurisdiction over their nationals; third, protective, by which states claim jurisdiction over those whose activities threaten their security or vital interests; fourth, passive personality, by which they claim jurisdiction over those who might threaten their nationals, even if they are abroad; and fifth, universality, under which all states may claim jurisdiction over those who have committed certain universally condemned crimes, such as piracy.[176] An extended discussion of prescriptive jurisdiction is beyond the scope of this report, but it seems obvious that an attack against U.S. systems would fall within U.S. prescriptive jurisdiction, even if its perpetrators were beyond the reach of U.S. authorities.[177]

Third, virtually all extradition treaties contain a "double criminality" requirement that mandates that the act that is the basis for the extradition request be an offense under the laws of both the requesting country and the one to which the request is directed.[178] This requirement has been a significant obstacle to U.S. efforts to try those who have intruded into sensitive U.S. data systems. In the case of computer hackers from the Netherlands who broke into U.S. Navy and NASA systems during the Persian Gulf War, for example, Dutch concepts of privacy were such that the hackers' intrusion into sensitive systems was not yet considered a crime under Dutch law.[179] Similarly, when Julio Caesar Ardita, a young Argentine, broke into computers containing sensitive information at the Naval Command Control and Ocean Surveillance Center, the Navy Research Laboratory, and Los Alamos National Laboratory, among others, the United States was unable to obtain his extradition, even though Argentine police cooperated with U.S. authorities, because Argentina's legal system, faced with new technology, had not yet classified such intrusions as criminal.[180]

The dual criminality requirement has, perhaps, also protected U.S. nationals who have been combatants in a different form of information conflict, namely the conflict surrounding the spread of U.S. popular culture. For example, when a Pakistani cleric recently reportedly asked the U.S. Department of State to extradite the entertainers Madonna and Michael Jackson because the lasciviousness of their performances violated Islamic law, the United States had no obligation to comply because, among other reasons, such violations of Islamic law are not criminal offenses in the United States.[181]

Lastly, most extradition treaties contain exemptions for "political offenses," although governments interpret that term differently. Some states will refuse extradition only

where the crime for which extradition is sought is a "pure" political offense, one directed at a sovereign political institution, absent the elements of common crime. Others refuse extradition for offenses committed in connection with a political cause or national liberation struggle. Some other states require that the political elements of the offense predominate over the common criminal elements. Finally, the French interpretation of the political offense exception is broader; French courts tend to deny extradition when a state wishes to punish an offender for injuries inflicted upon that state.[182] Whatever interpretation they embrace formally, many states will find rationales to deny extradition for those accused offenders whom they do not wish to extradite.

A country's extradition requests for those who have attacked it from abroad may fail for several reasons distinct from the aforementioned requirements. First, a country that supported an attack will have tremendous, obvious incentives not to extradite its agents and may take advantage of any loophole it can find. Such loopholes may include the requirements discussed above, as well as the prohibition in many countries' domestic laws against extradition of their own nationals. For example, in rejecting the U.S. and UK requests that it extradite the agents who were alleged to have carried out the Lockerbie bombing, Libya claimed that its law prohibited the extradition of its nationals and said that it planned to try them itself, fulfilling its obligations under the Montreal Convention.[183]

Second, as has apparently been the case with some terrorists, governments may reject extradition requests out of fear that the alleged criminals' colleagues will retaliate against them for their cooperation. In 1977, for example, France released Abu Daoud, the architect of the 1972 Munich Olympic massacre, despite efforts of the Federal Republic of Germany and Israel to obtain his extradition, apparently because it feared retaliation.[184] Similarly, after two Germans were taken hostage in Beirut, West Germany used the political offense exception in its extradition treaty with the United States and released Mohammed Ali Hamadei, whom the United States had indicted for hijacking TWA flight 847 in 1987.[185] Where information attacks with broad effects may be carried out from a distant sanctuary, the threat of such retaliation would appear particularly grave, especially for Western or other developed nations with significant dependence upon information infrastructures.

Third, the United States and other countries with advanced, vulnerable information infrastructures may exert diplomatic or other pressure to close some of the above loopholes, especially the failure of many countries' legal codes to recognize certain forms of computer intrusions as crimes. Nevertheless, potential incentives exist for countries to refuse to join any such formal or informal regime. First, of course, some countries may wish to use such intrusions or other attacks for their own political, economic, or other ends, and they may value maintaining that offensive capacity more than they do the incremental security that their systems would receive, particularly where their systems are poorly developed or relatively unimportant. Secondly, it is conceivable, although perhaps unlikely, that some nations may have ideological reasons to resist such rules, such as differing conceptions of privacy in electronic systems or data, or distrust of any system that would appear to preserve the advantages of the developed nations.[186] Finally, and perhaps most disturbingly, countries may choose not to criminalize certain conduct

as part of a development strategy. In what could be termed a form of "regulatory arbitrage,"[187] nations that hope to improve their information technology development may permit the behavior of hackers or other attackers in the hope that they will relocate to these nations, bringing with them their technical expertise. Such countries may seek the skilled personnel either to deploy them against enemies or to build their own economy or infrastructure.

Although the concept of "regulatory arbitrage" may seem farfetched, it should not be dismissed out of hand. First, it seems likely that countries, as well as transnational criminal organizations and, perhaps, terrorist groups, have sought individuals or groups of foreign hackers to engage in espionage, crime, or other attacks and that such recruitment will occur in the future. During the 1980s, for example, the Soviet Union employed a group of West German computer hackers, who were eventually apprehended after they broke into a series of U.S. civilian and military computers in search of U.S. and NATO defense secrets.[188] Second, "regulatory arbitrage" has taken place in other contexts. For example, in the wake of the U.S. military and diplomatic withdrawal after the Cold War, the Seychelles, hoping to attract foreign capital, enacted an Economic Development Act that granted citizenship and immunity from asset forfeiture or extradition to anyone investing at least $10 million in the islands.[189] Closer to home, the legislatures of several U.S. states have, at times, engaged in a "race to the bottom," weakening their restrictions on the conduct of corporate officers and directors in the hope of attracting corporations to register in their respective states.[190] States and countries have also given special incentives, reducing taxes and regulations or providing other benefits, in the hope of attracting business, including professional sports franchises.

Where a government refuses to extradite those responsible for attacks against another country, the victim state is not without recourse, although some options facing it may not be particularly attractive. First, of course, it may exert diplomatic, economic, or multilateral pressure against an uncooperative state, as has been the unsuccessful case with Libya after the Lockerbie bombing. Second, it may attempt to capture the alleged culprits and bring them back home for trial.

A government may contemplate abductions of criminal suspects from foreign lands when the urgent need to try the suspects outweighs the diplomatic and precedential costs of the abduction, and where such abductions do not violate the government's domestic law (if the government cares about such niceties). Abduction of suspects from foreign lands is not illegal under U.S. law, nor, at least, does it deprive U.S. courts of their ability to try abductees. In 1990, for example, after the Mexican government was unwilling or unable to extradite Dr. Humberto Alvarez-Machain, who had been indicted in a U.S. court for his role in the torture and murder of Enrique Camarena-Salazar, a U.S. Drug Enforcement Administration agent, U.S. agents abducted Dr. Alvarez-Machain and returned him to the United States for trial. The U.S. Supreme Court ultimately held that neither general principles of international law nor the terms of the U.S.-Mexico extradition treaty barred his prosecution, and that forcible abduction does not deprive a court of the ability to consider the case against the suspect.[191] Eventually, though, charges against Alvarez-Machain were dismissed for lack of evidence.

Depending upon the language of the applicable extradition treaty, such abduction will not violate its terms and, under the maxim male captus, bene detentus, international law recognizes the right of a state to try a suspect, even where his capture was technically illegal.[192] Nevertheless, agents operating abroad to capture suspects do violate the sovereignty of the countries in which they operate and risk punishment, perhaps for espionage or kidnapping, if they are apprehended by those countries' authorities. Furthermore, in the wake of the international and domestic furor that followed the abduction of Alvarez-Machain and the Supreme Court opinion permitting the abduction, such abductions seem likely to be extremely rare.

Retaliation

Responding to an "armed attack." Where a state can tie an attack to a foreign government, it may need to retaliate, either to terminate an ongoing attack or to prevent future attacks. The retaliating state would probably justify its retaliation as part of its right of self-defense as set out in Article 51 of the UN Charter. However, it is not obvious that Article 51 actually provides a basis for military action against a state conducting certain information attacks.

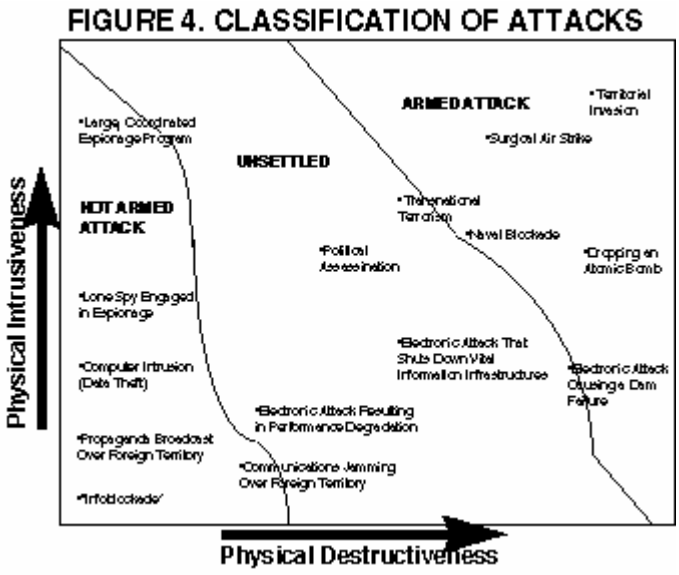
As discussed above, the peaceful settlement of disputes is one of the primary purposes of the United Nations Charter.[193] The Charter forbids the threat or use of force by one state against the territorial integrity or political independence of another state.[194] The only lawful use of force, besides collective action to enforce peace under UN auspices, is in individual or collective self-defense against "armed attack."[195] As the International Court of Justice asserted in its opinion in the case of Nicaragua v. United States, states do not have a right of armed response to acts which do not constitute an "armed attack."[196] A computer network-based attack, or one involving software weapons such as viruses, would not unquestionably qualify as "armed attack" under the UN Charter, and thus might not provide the international legal basis for a conventional, kinetic military response.

The UN Charter does not define "armed attack"; nor has the International Court of Justice (ICJ) laid out any comprehensive definition. To the extent that the term has been construed, it seems to include the use of armed forces, force, or violence, as well as interference with a nation's sovereign rights. Economic coercion does not constitute "armed attack" nor, for that matter, according to the ICJ, did the Nicaraguan Sandinista government's actions in providing sanctuary and support during the early 1980s to the rebels who fought the U.S.-backed government of El Salvador.[197] Even actions using destructive physical force may not rise to the level of "armed attack." Despite repeated requests, the United Nations refused to recognize guerrilla and terrorist attacks by Palestinians against Israel during the late 1960s and early 1970s as armed attacks, rejecting the Israeli position that individual small attacks from bases in Lebanon should be considered on a cumulative basis, as parts of an "armed attack" justifying Israeli incursions into Lebanon.[198]

As discussion of such terms as "war," "aggression," and "force" have shown, it can be difficult to predict whether specific actions will be considered to be "armed attacks." Unlike the domestic criminal law, international law sets out no mandatory elements of

"crimes," and any determination in such forums as the United Nations will be inherently political and diplomatic.[199] Nevertheless, it appears likely that an "armed attack" would include some level of actual or potential physical destruction, combined with some level of intrusion into its target's borders, or violation of its sovereign rights. Figure 4 is a rough attempt to predict potential categorization of information warfare attacks.

FIGURE 4



Some attacks, such as aerial bombing strikes against a nation's military command and control centers, are highly likely to be considered "armed attacks," as they involve high levels of both intrusion and destruction. Other attacks, such as propaganda broadcasts, are unlikely to be considered "armed attacks," at least by relatively impartial world forums. Attacks such as computer intrusions or communications disruptions are much harder to characterize. It may be that increases in one variable may make up for limitations in the other. For example, computer intrusions for purposes of stealing data and to disrupt air traffic control may be equally intrusive, but the greater level of destruction and death that the air traffic control system attack may cause may make it more likely to be considered "armed attack" than would the data theft attempt. Furthermore, attacks that are sufficiently destructive may qualify as "armed attacks," no matter what their level of intrusion, and vice versa.

If a target country cannot characterize a computer attack against its information systems as an "armed attack," then it may not be able to respond to the attack with conventional, kinetic force, unless it wants to risk having its response considered the aggressive "armed attack" under Article 51. Presumably, a response in kind would not constitute "armed attack" if the original attack did not, but some potential information attackers, who may be able to hire from abroad the equipment and expertise they need for their attacks, may lack the information infrastructures to make them vulnerable to such attacks.

Proportionality. In addition to the United Nations' requirements that force be limited to a response to an armed attack, customary international law has developed requirements for

retaliation. Such retaliation must be in individual or collective self-defense against an attack; it must be necessary to stop the initial, unjustified attack or to prevent further violations; and it must be proportional to the attack to which it is a response.[200]

The proportionality analysis applies in two ways. First, under the requirements of the jus ad bellum, the level of force of the response must be proportionate to that of the initial attack-a full-scale blitzkrieg across a broad front accompanied by aerial bombing would generally be disproportionate to a patrol's border raid, for example. Second, as in any other military action, the response must balance the damage it will inflict, especially to civilians, against the military objectives it is intended to accomplish.[201]

Just as it is not obvious that an information attack will be an "armed attack," it is not obvious what would be proportionate to such an attack, especially where the attack inflicts little or no physical destruction or loss of life. Where a computer intrusion disrupts or corrupts a database or denies service for important elements of the electronic infrastructure, inflicting great hardship on the target country, that country must determine what sort of response would be proportionate to the attack. In the absence of real physical destruction or death, such as by the crash of a passenger aircraft through manipulation of the air traffic control system, it is questionable that a conventional military attack would be proportionate. The use of force may be qualitatively distinct from other tools of coercion, as demonstrated by its inclusion in the UN Charter and the UN definition of aggression.[202]

If a conventional response is disproportionate to an information warfare attack, a response in kind could seem likely to be proportionate. However, such a response may require the use of neutral assets, such as networks owned by or passing through neutral countries and thus could run the risk of violating their neutrality.[203] Perhaps more significantly, because of the limited infrastructure and resources necessary to conduct some information warfare attacks, and the potential expertise available for hire or ideological recruitment, an adversary who has attacked the United States or a similarly advanced country may lack sufficient targets for an information warfare response, or may have only targets that are too important to be retaliated against for anything other than a grave attack. It would seem inappropriate to cause aircraft to crash, for example, in retaliation for a limited disruption of a local telephone network, or an intrusion into a military computer.

It seems unlikely that the United States would refrain from traditional military retaliation where an information warfare response would be inappropriate overkill or ineffectual underkill. It also seems unlikely that international law would mandate such inaction. Assuming that an information warfare attack is an "armed attack," and an information warfare response were unavailable or excessive, then a kinetic response, appropriately calibrated, would seem proportional even if, as a general rule, the relevant form of information warfare attacks were considered distinct from violence.[204] If the information warfare attack is not an "armed attack" justifying a military response under the UN Charter, then, aside from such measures as economic sanctions, the United States might then assert an underlying, inherent right of national self-defense, which predates and goes beyond the rights contained in Article 51 of the UN Charter,[205] rather than suffering

ongoing attacks stoically or petitioning the UN Security Council for help. In considering their responses to such attacks, policymakers must be aware that their actions may establish precedents that other nations may look to in similar circumstances, or draw upon cynically to excuse their behavior in dissimilar circumstances.

In sum, current understandings of "armed attack," as well as dissonance between international networks and the international system of state sovereignty, may complicate or hinder victims' efforts to respond to information warfare attacks. The United States may need to pursue international initiatives to change that understanding, as well as to alter nations' responsibilities, or lack thereof, to forego such attacks, prevent their occurrence, or to cooperate in defensive or law enforcement measures.

Chapter 4: Conclusion—Reconciling Technology and International Law, Resolving Ambiguities, and Balancing Capabilities

As discussed above, international law has not yet resolved ambiguities over the characterization of information warfare activities, and must face a conflict between the international system of sovereign states and the realities of global networks. International law thus leaves space for the United States and others to conduct information warfare activities, perhaps even in peacetime, without significant legal repercussions. Conversely, international law may permit attacks against the United States, as well as exacerbate U.S. difficulties in responding to attacks against it, particularly in peacetime.

The legal status quo may appear satisfactory to U.S. policymakers. As the United States apparently leads the world in information warfare development, an international legal regime that permits information attacks can give it an advantage, allowing the United States to apply its technological strength to international conflicts in ways beyond the capacities of anyone else. In the absence of conclusive legal authority indicating, say, that particular information warfare attacks are "armed attacks," "aggression," or "force," the United States can act with some confidence that its acts will not be held to be so. Given its position in the world, the United States will have the opportunity to begin the state practice that can establish international norms and, perhaps, customary international law. To an extent, then, given the United States' voice in world politics and predominant military might, the United States is in the positions of legislator, sheriff, and (perhaps, to its adversaries) executioner, and it has a lot of influence over the judge.

Despite its freedom to act, the United States should not be sanguine about the state of international law. The "legislator, sheriff, and executioner" may all live together in a large glass house. Just as the United States can attack, it can be attacked, and its actions in conducting attacks may provide precedent for attacks against it and its allies. Furthermore, just as U.S. capabilities may outstrip those of its potential adversaries, so too may its vulnerabilities, as it is perhaps uniquely dependent upon its information infrastructure for both civilian and military needs. If only to increase protection for U.S. systems, then, certain nonexclusive legal, diplomatic, or policy initiatives may be appropriate.

Resolution of Legal Ambiguities

A first approach would be to clarify the delineation of such terms as "armed attack," "force," and others, so that the status of information warfare attacks under international law is understood. Without knowing the extent of U.S. offensive capabilities or defensive vulnerabilities, it is impossible for us to judge the desirability of limiting information warfare.[206] The United States might support restrictive definitions of those terms, so as to preserve its ability to use its technological advantages, to protect potentially desirable technological developments, and to encourage the use of nonlethal methods of conflict; or it might support broad definitions, to help reduce the lawful methods by which adversaries can exploit its vulnerabilities. Definitions that included nonlethal information

warfare attacks within "war" or "force" could give civilians a measure of protection from such attacks during times of peace, as they would increase the diplomatic and political repercussions of such attacks. To protect civilian targets during wartime, the United States could pursue treaties or other international understandings that the financial or other intangible damages caused by certain types of nonlethal information attacks are, indeed, the types of injuries against which humanitarian law should protect noncombatants.

The United States may use several legal mechanisms to achieve the goal it chooses, ranging from a treaty setting out the circumstances in which certain types of information warfare are permissible, to silence on the subject to avoid hindrances on U.S. capabilities. Additionally, the United States could try to influence the development of customary international law regarding the appropriateness of information warfare. It may move for declarations of the UN General Assembly interpreting the Charter as it would apply to information warfare.[207] U.S. statements of its views on the subject would have a significant effect both on the opinions of other states and, ultimately, the emergence of international norms regarding information attacks, or particular aspects thereof. Although customary international law traditionally evolved naturally from state practice over an extended period of time, states have recently pursued efforts to create customary law purposefully. Such efforts have been most visible in international forums, such as the General Assembly, which has passed declarations setting out world opinion as to the state of the law on such topics as the use of nuclear weapons, seabed mining, or the equation of Zionism with racism. [208]

There is no reason, though, that an individual state could not set out to influence the development of customary legal norms, especially in an area such as information warfare, where that state leads the world in the development or application of the technologies and techniques to which these norms would be applied. U.S. efforts to draw world attention to dangers that information warfare poses could be counterproductive, however, as they might spur other countries' efforts to obtain or use information warfare weapons, and those countries may be suspicious of what they perceive to be U.S. efforts to protect its technological advantages or retard the development of others' capacities.

International Cooperation Against Computer Attacks

Second, to improve its defensive or responsive options, the United States could make efforts to reconcile the system of sovereign states with international networks, through promoting harmonization of laws and cooperation in investigation and prosecution of computer attacks. The first part of such a strategy would include diplomatic pressure and criminal justice advice and assistance to promote the criminalization of computer-based attacks in those nations that do not yet recognize such attacks as crimes, both to encourage other countries to discourage such behavior by individuals within their borders, and to enable extradition of offenders. Secondly, the United States could support the development of an extradition regime for criminal or terrorist computer attacks, obliging all countries to extradite or try those who have committed specified network-related crimes. Models for such measures could be drawn from the treaties executed in the 1960s and early 1970s to combat hijacking and other terrorism against civil

aviation.[209] The Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation, for example makes it an offense for anyone to destroy an aircraft, place a device likely to destroy an aircraft, destroy or damage air navigation facilities, or communicate information which he knows to be false, thus endangering the safety of aircraft in flight,[210] and it obliges countries to extradite or try suspected offenders. Such agreements, along with diplomatic and other public statements relating to the criminalization of such attacks, could also contribute to the development of a norm that countries cannot support computer-based attacks in peacetime, or that they must cooperate in resisting such attacks. Given the United States' and its allies' ambiguous success in fighting international terrorism, it is obvious, though, that such agreements or norms would not be panaceas.

Protection of Critical Systems

Third, just as the aviation efforts were incremental steps in the fight against terrorism, similar efforts could be made for the protection of particular information systems from dangers including crime, terrorism, war, or even natural disasters. Some systems may be so critical that countries can agree that they must be put off limits from attacks, or that all countries must cooperate to defend them. Systems that could be the subject of individual protection regimes include those involved in the command and control of strategic weapons, international financial transfers, individual financial markets or stock exchanges, telephone switches, emergency communications, rail transport, and medical databases.[211] Such arrangements could be pursued under direct UN auspices, or as individual treaties in the context of existing institutions, such as the ITU, OECD, or ICAO, or even, perhaps the World Intellectual Property Organization (WIPO).

Along with providing legal bases for responses and countermeasures, incremental prohibitions against certain information warfare attacks could contribute to the development of broader international norms against such attacks, particularly in peacetime. In the context of nuclear weapons, in comparison, proclamations and regional agreements against the use of nuclear weapons contributed to the legal argument that the use of such weapons had become illegal, although the International Court of Justice did not ultimately embrace that argument.[212]

Arms Control for Information Warfare?

A fourth approach that has been suggested could be to pursue some sort of ban on information warfare attacks or control of the weapons of information warfare.[213] Such an approach would seem to provide clear legal norms to guide future actions, and might seem particularly sensible if the United States were to determine that its vulnerabilities outweighed its technological advantages.

But such clarity would be illusory; the distinction between information warfare and traditional warfare is blurry, at best. An information warfare weapons ban would pose problems because not only do many information weapons have dual military and civilian uses, but their applications are predominantly civilian. Because of technological

diffusion, the small size of much information technology, and its primary incorporation into consumer goods, an arms control regime would seem difficult to enforce. Furthermore, although arms controls and weapons bans have been applied to new technologies before they were widely used or their military ramifications understood, as in the bans on bacteriological weapons,[214] hostile use of environmental modification techniques,[215] and blinding laser weapons,[216] it does seem premature to limit a weapon that promises to bring some measure of nonlethality to conflict, and in which the United States apparently holds an advantage in development. In any event, arms controls or warfare bans would not apply to the non-state actors, such as terrorists or criminal organizations, who would not be parties to the agreements and who may make up the gravest short-term information warfare threat. Such bans, then, would not eliminate the need for defensive measures, so countries might still need to explore offensive capabilities, if only to test their defensive measures adequately.

The Lure of Inactivity

A final prospective course of action is to do nothing, or very little. Although international law does not now conclusively address the legality of many information warfare attacks or the appropriate responses to them, that has not been a grave problem yet, because the attacks, aside from some computer intrusions and crimes, have not been particularly serious. But as information technology continues to develop and diffuse, the danger of such attacks seems likely only to increase, as might the opportunities for U.S. offensive uses. If the United States needs to conduct such attacks, it will undoubtedly do so. If the United States is subject to attacks, it will respond. International law will address information warfare attacks in some way or another. It may be wise to address the legal issues that the United States will face in advance, rather than having to address them in the heat of an emergency, where inadequate legal institutions may reduce national options and precedents may be set by exigencies, rather than forethought.

Conclusion: A Caveat

Despite the apparent attractiveness of addressing the potential international legal issues arising from the development of information warfare technologies and techniques before the issues actually arise, it is important to remember (and easy for lawyers to forget) that law is no panacea. Even the wisest agreements and soundest legal analysis will not guarantee the safety of U.S. systems or the potency of U.S. offensive measures. Law can go a long way toward regulating nations' and individuals' behavior, and it can be an important part of diplomatic efforts both to alleviate conflict and to address its effects. At the same time, though, the development of advanced information warfare technologies and techniques and the continuing global diffusion of information technology illustrate the fluidity of the world that law attempts to govern. No law can change as swiftly as can technology; unless law is to somehow stop technology's seemingly inexorable worldwide progress, it cannot fully control the use of its fruits for warfare. Legal measures can thus supplement, but not supplant, vigilance, preparedness, and ingenuity.

About the Authors

Lawrence T. Greenberg is General Counsel of The Motley Fool, Inc., a provider of investor information and education through various media, including the Internet and on-line services. Before joining The Motley Fool, he spent 1995-96 at the Project on Information Technology and International Security at the Stanford University Center for International Security and Arms Control. He has worked as an attorney for the National Security Agency and at the Silicon Valley law firm of Wilson, Sonsini, Goodrich & Rosati, where he specialized in securities and intellectual property. A member of the state bars of Texas and California, he clerked for Judge Jerry E. Smith of the U.S. Court of Appeals for the Fifth Circuit. He holds an A.B. in government from Harvard College, an M.A. in political science from Stanford University, and a J.D. from Stanford Law School.

Seymour E. Goodman is the director of the Project on Information Technology and International Security at the Stanford University Center for International Security and Arms Control, and Professor of MIS at the University of Arizona. Professor Goodman studies the international dimensions of information technologies and related public policy questions. He has chased after computers on all 7 continents and in about 70 countries. He was an undergraduate at Columbia University and received his Ph.D. from the California Institute of Technology.

Kevin J. Soo Hoo is a Ph.D. candidate in the Department of Engineering Economic Systems and Operations Research at Stanford University. He received a B.S. in Electrical engineering from Santa Clara University.

Endnotes

[1] Cf. Alvin Toffler & Heidi Toffler, War and Anti-War 2 (1993) ("the way we make war reflects the way we make wealth").

[2] U.S. Department of the Air Force, Cornerstones of Information Warfare (1995) at 2. For other definitions of information warfare see, for example, Richard W. Aldrich, The International Legal Implications of Information Warfare, U.S. Air Force Institute for National Security Studies Occasional Paper 9, (April, 1996) at 3-5. The Air Force's definition is particularly suitable for this report, which attempts a broad examination of potential legal issues.

[3] See, e.g., Douglas Waller, Onward Cyber Soldiers, Time, Aug. 21, 1995, at 37.

[4] E.g., Charles J. Dunlap, How We Lost the High-Tech War of 2007, The Weekly Standard, Jan. 29, 1996 at 22.

[5] John Arquilla & David Ronfeldt, The Advent of Netwar (1996)

[6] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, Strategic Information Warfare: A New Face of War 64 (1996). One observer has suggested that in the late 1960s, U.S. agents altered AT&T telephone switching equipment that was exported to Poland, so that the U.S. could shut down land based telecommunications on command. Winn Schwartau, Export Control as a Proactive Defensive Information Warfare Mechanism, available at http://www.infowar.com/mil_c4i/export.html.ssi.

[7] Molander, supra note 6, at 64.

[8] Id., at 66.

[9] Neil Munro, Pentagon Developing Cyberspace Weapons, Washington Technology, June 22, 1995.

[10] Peter Grier, Information Warfare, Air Force Magazine (March 1995) 34, 35.

[11] Barry Collin, Terrorism and the New World Disorder, 11th International Symposium on Criminal Justice Issues, Office of International Criminal Justice, The University of Illinois at Chicago, 1996.

[12] In September of 1996, anonymous e-mail messages overwhelmed network routers in the U.S. Northwest, disrupting regular e-mail delivery for almost six hours. Seattle Times, Oct. 11, 1996, at A1, Edupage, October 16, 1996.

[13] Molander, supra note 6, at 74

[14] In 1988, a worm created by Robert Morris, a Cornell University graduate student, spread over the Internet to thousands of computers, including some military and

intelligence systems, paralyzing over 6,000 computers. Steve Lohr, Ready, Aim, Zap, N.Y. Times, Sept. 30, 1996, at D1, D2.

[15] Sean P. Kanuck, Recent Development, Information Warfare: New Challenges for Public International Law, 37 Harv. Int'l. L.J. 272, 289 (1996).

[16] See, e.g., Tom Clancy, Debt of Honor (1994).

[17] Vienna Convention on the Law of Treaties(1969), UN doc. A/CONF.39/27. A third source of international law is jus cogens, peremptory norms that have the character of supreme law and which cannot be modified by treaty or ordinary customary law. Id., Art. 53, 64. Louis Henkin, International Law: Politics and Values 38-39 (1995). Although no satisfactory way to identify jus cogens exists, some have argued that it prohibits (although perhaps not effectively) genocide, slavery and the slave trade, and apartheid.

[18] Henkin, supra note 17, at 28.

[19] Id., at 29-38.

[20] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart J., concurring).

[21] E.g., Frank H. Foster & Robert L. Shook, Patents, Copyrights, and Trademarks (2d ed. 1993) 182.

[22] Jonathan A. Charney, May The President Violate Customary International Law?: The Power of the Executive Branch of the United States Government to violate Customary International Law, 80 Am. J. Int'l L. 913, 914 (1986).

[23] Macbeth, Act V.

[24] Mark W. Janis, An Introduction to International Law 1 (2d ed. 1993)

[25] See Parts II.C., III. E.2.a , infra (Discussions of "force" and "armed attack").

[26] An "infoblockade" requiring the use, or denial, of third countries' assets or territory might require those countries' consent, or might violate their borders. See Part II.B.1, infra.

[27] Although a naval blockade would generally not violate a nation's borders, it would constitute a physical disruption of a nation's sovereign rights to freedom of the seas, which could be considered analogous to the border intrusion.

[28] See Part II. B. 2., infra.

[29] Although the U.S. Constitution only explicitly makes treaties part of U.S. law, the U.S. Supreme Court appears to have included customary law within the law of the land. U.S. Const., Art. VI; The Paquete Habana, 175 U.S. 677, 700 (1900) ("International law is part

of our law, and must be ascertained and administered by the courts of justice of appropriate jurisdiction . . "). Henkin, supra note 17, at 68-71

[30] This report does not address issues arising under U.S. domestic law, or the domestic laws of other countries. Such issues would include the source and allocation of authority for defense and offensive measures during both war and peace, the allocation of liability for protection of critical infrastructures, and the potential conflict between individual liberties (including freedom of expression under the First Amendment to the U.S. Constitution) and national security. For a discussion of the application of some U.S. domestic law to information warfare activities, see Science Applications International Corporations, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (July 4, 1995).

[31] See Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. ___ 21 (July 8, 1996) (hereinafter, "Advisory Opinion").

[32] Advisory Opinion, 86.

[33] Although founded well before the establishment of the United Nations, the ITU is now part of the UN system.

[34] 1 Gerd D. Wallenstein, International Telecommunications Agreements 67-69 (1986).

[35] Harold M. White, Jr. & Rita Lauria, The Impact of New Communication Technologies on International Telecommunication Law and Policy: Cyberspace and the Restructuring of the International Telecommunication Union, 32 Cal. W.L. Rev. 1 (1995).

[36] George A. Codding, The International Telecommunication Union 84-87 (1952). Even the Titanic disaster might have been avoided, or more of its passengers rescued, but for Marconi employees who refused communications from operators using non-Marconi equipment. White & Lauria, supra note 35, at 6.

[37] International Telecommunications Convention (hereinafter "ITC"), Art. 35.

[38] Sara Anne Hook, Comment, Allocation of the Radio Spectrum: Is the Sky the Limit? 3 Ind. Int'l & Comp. L.R. 319, 325 (1993).

[39] ITC, Art. 38.

[40] Radio Regs Art. 18, Sec. 2(c). 4 Umberto Leanza, The Future of International Telecommunications (1992).

[41] Radio Regs Art. 18, Howard A. Bender, Note, The Case of the Sarah: A Testing Ground for the Regulation of Radio Piracy in the United States, 12 Fordham Int'l L.J. 67, 69 (1988). This prohibition does not apply to the truth or falsehood of the underlying substance of a transmission but to the identification of its transmitter and frequency.

[42] ITC Art. 22 sec. 1.

[43] ITC Art. 19.

[44] Radio Rules (1923).

[45] 1 Wallenstein, supra note 34, at 30-31.

[46] Audrey L. Allison, Meeting the Challenges of Change: The Reform of the International Telecommunication Union, 45 Fed. Comm. L.J., 491, 514 (1993); Hook, supra note 38, at 328; Christian A. Herter, The Electromagnetic Spectrum: A Critical Natural Resource, 25 Nat. Resources J. 651, 658 (1985).

[47] Kanuck, supra note 15, at 289 n.73; Stephen Gorove, Developments in Space Law 49 (1991) ("While states generally abide by ITU resolutions, they are not legal bound by them." See Part III.E.2.a., infra (discussion of "armed attack").

[48] Art. IV.

[49] Art. 3(3)

[50] Art. 3(1); Glenn Harlan Reynolds, International Space Law: Into the Twenty-First Century, Vand. J. Transnat'l L. 225, 230 (1992). The United States, among other spacefaring powers, has not ratified the Moon Treaty.

[51] 10 I.L.M 909.

[52] 31 U.S.T. 1, 1143 U.N.T.S. 105.

[53] The use of nuclear weapons in space to generate electromagnetic pulses (EMP) would seem to be forbidden, however.

[54] See Colleen Driscoll Sullivan, The Prevention of an Arms Race in Outer Space: An Emerging Principle of International Law, 4 Temp. Int'l & Comp. L.J. 211, 230-34 (1990).

[55] Reynolds, supra note 50 at 241.

[56] Sullivan, supra note 54 at 213-14

[57] See, infra Part III. C., and Part III. E. 2. a. (discussions of "force" and "armed attack").

[58] See Reynolds, supra note 50, at 241 (unclear whether space-based lasers would count as "weapons of mass destruction"). See also John M. Orr, Comment, The Treaty on Outer Space: An Evaluation of the Arms Control Provisions, 7 Colum. J. Transnat'l L. 259 (1968).

[59] Aldrich, supra note 2, at 20.

[60] Advisory Opinion 64.

[61] Kanuck, supra note 15, at 276; Abram N. Shulsky, Silent Warfare: Understanding the World of Intelligence 103 (2d ed. 1993)

[62] Reynolds, supra note 50 at 239-41; Mark Orlove, Spaced Out: The Third World Looks for a Way in to Outer Space, 4 Conn. J. Int'l L. L. 597, 629-32 (1989).

[63] A 1923 U.S.-British Claims Arbitration Tribunal granted no compensation to the British cable company whose Manila-Hong Kong cable the U.S. had cut during the Spanish-American War. Ranier Lagoni, Cables, Submarine, 1 Max Planck Institute for Comparative Public Law and International Law, Encyclopedia of Public International Law 516, 517-19 (1992).

[64] Id.

[65] Lagoni, supra note 63, at 517

[66] E.g., Protocol Additional to the Geneva Conventions of 12 August 1949; and Relating to the Protection of Victims of International Armed Conflicts (1977) (hereinafter Additional Protocol I). Although the United States has not ratified the Additional Protocol, the protocol reflects much customary and conventional international law. Advisory Opinion at 84.

[67] Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907) (hereinafter "Hague V"), Art. 1.

[68] See United Nations Manual on the Prevention and Control of Computer-Related Crime, 261-264 (1993) (hereinafter "UN Manual").

[69] See Part III. C., infra.

[70] Hague V, Art. 2, 5. Similarly, under the unratified 1925 Hague Air Warfare Rules neutrals were obliged to prevent the entry of belligerent military aircraft into their airspace, compel their landing, and prevent their departure .

[71] Hague V, Art. 3, 5.

[72] Hague V, Art. 8.

[73] Hague V, 1923 Radio Rules.

[74] 1 Howard S. Levie, The Code of Armed Conflict 123 (1986).

[75] Such law includes the Geneva Convention of 1949, The Hague Convention (IV) Respecting the Laws and Customs of War on Land (1907) (hereinafter "Hague IV"), the Genocide Convention, and the Nuremberg Charter. Advisory Opinion 81.

[76] Advisory Opinion 77

[77] Advisory Opinion 86

[78] Judith Gail Gardam, Proportionality and Force in International Law, 87 Am. J. Int'l L. 391, 396 (1993).

[79] Hague IV, Art. 25

[80] Statute of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia Since 1991 (1993) (hereinafter, "Yugoslavia Tribunal").

[81] No defendants were convicted of such bombing at Nuremberg. Given the extent of the Allied bombing of Germany and Japan, such convictions might have seemed hypocritical; this omission, though, may have undermined the viability of this principle of international law. See Howard S. Levie, Terrorism in War: The Law of War Crimes (1992). Nevertheless, the Nuremberg tribunal reaffirmed that attacks directed at civilians as civilians was illegal. George Bunn, US Law of Nuclear Weapons, 32 Naval War College Rev. 46, 58 (1984). The inclusion of indictments for attacks against civilians in the Charter of the Yugoslavia tribunal further attests to some measure of survival of the principle.

[82] Additional Protocol I, 52(2).

[83] Advisory Opinion 78; Gardam, supra note 78, at 410.

[84] See discussion of proportionality in response to attacks, Part III. E. 2. b., infra.

[85] Gardam, supra note 78, at 391.

[86] Id., at 407-08; Committee on International Arms Control and Security Affairs & Committee on International Law, The Use of Armed Force in International Affairs: The Case of Panama, 47 Rec. Assoc. Bar City N.Y. 604, 683-84 (1992).

[87] Hague II, Hague IV, Additional Protocol I.

[88] See, e.g., Saint Petersburg Declaration of 1868 (only legitimate object of war is to weaken enemy's military forces); Nuremberg Charter (prohibition against "wanton" bombing; Hague IV, Art. 25 (prohibition against bombardment "by whatever means" of undefended towns, dwellings or buildings); Yugoslavia Tribunal.

[89] See Additional Protocol I, Art. 54(1) (starvation may not be used as tool of war).

[90] Aldrich, supra note 2 at 11.

[91] James Winnefeld, Preston Niblack & Dana Johnson, A League of Airmen: U.S. Airpower in the Gulf War 205 (1994).

[92] Eric J. Sterner, Digital Pearl Harbor, National Security in the Information Age, National Security Studies Quarterly (Summer 1996) 33, 43.

[93] Kanuck, supra note 15, at 284.

[94] Information Revolution Spawns "Revolution in Security Affairs," Defense Daily, June 8, 1995, at 1.

[95] See Additional Protocol I, Art. 56 (dangerous forces).

[96] Richard Szafranski, A Theory of Information Warfare: Preparing for 2020, Airpower Journal (Spring 1995).

[97] See Colonel Brenda J. Hollister, USAF, The Thomas P. Keenan, Jr. Memorial Lecture: The International Criminal Tribunal for Yugoslavia, 39 A.F. L. Rev. 37, 40 (1996) (incitement to genocide in former Yugoslavia as a war crime); J. Balzar, The Power of Africa's Airwaves, L.A. Times (Oct. 22, 1995) A1 (relationship between hate radio and Rwandan genocide).

[98] Michael N. Schmitt, State Sponsored Assassination in International and Domestic Law, 17 Yale J. Int'l L. 609, 617 (1992).

[99] Additional Protocol I, Art. 37.

[100] Hague IV, Art. 23. The provision only applies to the use of enemy uniforms in combat. Trial of Skorzeny and Others, 9 W.C.R. 90, 93-94 (U.S. Zone-Germany, Gen. Mil. Gov. Ct. 1947). Although Additional Protocol I, Art. 39(2) bars the use of enemy uniforms for purposes other than attack as well, the United States, which has not ratified the Protocol, resists that provision as nonreflective of the nature of modern combat. Schmitt, supra note 90, at 636.

[101] This example was suggested by Professor Daniel T. Kuehl of the National Defense University.

[102] E.g., Reynolds, supra note 50, at, at 239; Orlove, supra note 62, at 629-32.

[103] E.g., Gary H. Anthes, New Laws Sought for Information Warfare as Technology Outpaces the Law, Computerworld, June 5, 1995, at 1.

[104] The leading U.S. law dictionary defines "war" as "Hostile contention by means of armed forces, carried on between nations, states, or rulers, or between citizens in the same nation or state." Black's Law Dictionary (6th ed. 1990) 1583, citing Gitlow v. Kiely, 44 F.2d 227, 233 (S.D.N.Y. 1930).

[105] Clinton E. Cameron, Note, Developing a Standard for Economically Related State Economic Action, 13 Mich. J. Int'l L. 218, 219 (1991).

[106] Amendments of the Brazilian Delegation to the Dumbarton Oaks Proposals, Doc. 2, 617(e)(4), 3 U.N.C.I.O. Docs 251, 253-54 (1945). Part of the reason for the proposal's defeat may have been the argument that economic measures were included in Article

2(4)'s language referring to pressure in any manner "inconsistent with the purposes of the United Nations." Cameron, supra note 105 at 225.

[107] See Part III. E. 2 a., infra.

[108] G.A. Res. 3314 (XXIX) (December 14, 1974) (Hereinafter "Declaration on Aggression")

[109] UN Charter, Art. 39.

[110] Declaration on Aggression., Art. 1.

[111] Id., Art. 2.

[112] The phrase "the use of any weapons by a state against the territory of another" could be read as applying to the non-lethal tools of information warfare. However, because the provision in which it is included addresses bombardment by the armed forces, and because "weapon," too, connotes force or violence, this clause probably would not bring all of information warfare within the concepts of "war," "force," or "aggression." See, e.g., New American Webster Dictionary (1972), at 510 (defining "weapon" as "any instrument used in fighting.")

[113] Declaration on Aggression, Art. 3.

[114] Cameron, supra note 105, at 230.

[115] Advisory Opinion 85. See Theodor Meron, The Time Has Come for the United States to Ratify Geneva Protocol I, 88 Am. J. Int'l L. 678 (1994).

[116] Additional Protocol I, Art. 49(1); 1 Levie, supra note 74, at 33-34 (§ 151.2).

[117] Note, Judicial Determination of the End of the War, 47 Colum. L. Rev. 255 (1947) (hereinafter "Judicial Determination"); 7 Moore Digest of International Law (1906) 153. See also Hijo v. U.S., 194 U.S. 315 (1904) (cessation of hostilities is not legal termination of war).

[118] Joint Resolution of July 2, 1921, 42 Stat 105 (1921); Judicial Determination, supra note 117, at 257,

[119] UN Charter, Preamble.

[120] Id.

[121] Id., Art. I(1).

[122] Id., Art. I(2).

[123] Id., Art. I(3)

[124] Id., Art. 2(3).

[125] Id., Art. 2(4).

[126] G.A. Res. 2625, UN GAOR, 25th Sess., Supp. No. 28, at 121, UN Doc. A/8082 (1970); Cameron, supra note 105, at 235.

[127] G.A. Res. 2131, 20th Sess., Supp. No. 14, at 108, UN Doc. A/6014 (1965).

[128] Cameron, supra note 105, at 235.

[129] Kanuck, supra note 15, at 290-91.

[130] See notes 17-22 supra and accompanying text.

[131] Kanuck, supra note 15, at 289

[132] The sanctions that such a country might employ to such an end might, of course, implicate its obligations under such international agreements as the General Agreement on Tariffs and Trade (GATT), and could subject the country to international sanctions in response.

[133] See generally, Cameron, supra note 105, at, 242-243.

[134] Wade D. David, European Diplomacy in the New Eastern Question, 1906-1909, at 104 (1940).

[135] Cameron, supra note 105, at, 242-43

[136] M. Reza Ghods, Iran in the 20th Century 187-89 (1969).

[137] Andreas F. Lowenfeld, Trade Controls for Political Ends, 313-21 (2d ed. 1983).

[138] R.R. Baxter, The Law of International Waterways 168-183 (1966); Ranier Lagoni, Canals in 1 Max Planck Institute for Comparative Public Law and International Law, Encyclopedia of Public International Law 523, 526 (1992). A canal becomes internationalized when, by treaty, declaration, or otherwise it is declared open to free access and unimpeded navigation of ships of all nations. The Panama Canal, for example, was internationalized before its construction by the Hay-Pauncefote Treaty of 1901 between the U.S. and Great Britain. This internationalization was reasserted in the treaty by which the U.S. acquired the Canal Zone from Panama in 1903. Baxter, supra note 138 at 170-71; Louis Henkin, Richard Crawford Pugh, Oscar Schachter, Hans Smit, International Law Cases and Materials (3d ed. 1993) 1263-64.

[139] The covert nature of such acts, however, makes their contribution to international law suspect, and may actually reinforce the principle that such acts are illegal.

[140] See discussion of "armed attack," Part III. E. 2. a., infra.

[141] UN Charter, Art. 39.

[142] Id., Art. 41-49.

[143] See, e.g., notes 3 - 16 supra and accompanying text, supra.

[144] See, e.g., Kevin J. Soo Hoo, Seymour E. Goodman, and Lawrence T. Greenberg, Terrorism and the Information Revolution __ Survival ___ (1997) (forthcoming).

[145] Caroline Osborne, a British Crown Prosecutor, has characterized those who break into computer systems as "stupid little nerds who have not yet discovered girls and beer." Brian Foran, Information Warfare: Attacks on Personal Information, 8th Annual Canadian Security Symposium: Business and Security in an Electronic World, May 2, 1996.

[146] Norman Menachem Feder, Note, Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack, 19 N.Y.U.J. Int'l L. & Politics 393, 412 (1987).

[147] Mary Fackler Schiavo, "I Don't Like to Fly," Newsweek, May 20, 1996, at 27.

[148] Peter G. Neumann, Computer Related Risks 126-28 (1995). See also, M.E. Bowman, Is International Law Ready for the Information Age? 19 Fordham Int'l L.J. 1935, 1939-40 (1996).

[149] E.g., Cyber Wars, The Economist, (Jan. 13, 1996), at 77.

[150] Neumann, supra note 148, at 115.

[151] Id., at 37.

[152] See Stefan Geisenheyner, The Dangers Lurking in Military Software Production: Viruses, Trojan Horses and Logic Bombs, Armada Int'l, Oct.-Nov. 1989, at 22.

[153] Simson L. Garfinkel, The Manchurian Printer, The Boston Globe, Mar 5, 1995, Focus Section, at 83.

[154] See, e.g., Scott Sagan, The Limits of Safety (1993); Charles Perrow, Normal Accidents (1984)

[155] W. Michael Reisman, The Constitutional Crisis in the United Nations, 87 Am. J. Int'l L. 83, 86 (1993).

[156] Christopher C. Joyner & Wayne P. Rothbaum, Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law? 14 Mich. J. Int'l L. 222, 248 (1993).

[157] Id., at 252.

[158] Mark W. Janis, An Introduction to International Law 1 (2d ed. 1993).

[159] UN Manual, 265.

[160] ICJ Reports 1949 at 34-35.

[161] See International Working Group on Data Protection in Telecommunications, Data Protection on the Internet (21 May 1996), J. Information L. & Tech., Sept. 30, 1996, available at http://elj.warwick.ac.uk/elj/jilt/consult/iwgdp/1.htm#problems.

[162] UN Manual, 264.

[163] U.S. Permanent Subcommittee On Investigations, Committee on Governmental Affairs, Appendix "A" to Staff Statement (June 5, 1996) at 5-6. The North Korean government might not have found persuasive the argument that under international law such an attack might not constitute.

[164] See Hook, supra note 38, at 327; Herter, supra note 46, at 655.

[165] The Vienna Concluding Document of the Committee for Security and Cooperation In Europe (CSCE) meeting in 1987, in its discussion of "Human Contacts" stated that states were obligated to ensure that radio services operating in accordance with the ITU Radio Regulations can be received within their states. Peter Malanczuk, Information and Communication, Freedom of, 2 Max Planck Institute for Comparative Public Law and International Law, Encyclopedia of Public International Law 976, 986 (1992). Nevertheless, it seems unlikely that states have renounced the ability to attempt to jam foreign broadcasts within their borders.

[166] U.S. General Accounting Office, Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84 (May 1996) 22.

[167] Gary H. Anthes, Info-terrorist Threat Growing, Computerworld, Jan. 30, 1995, at 1. See also Bowman, supra note 148, at 1933. Even in the physical world, a country will not be held responsible for acts conducted on its territory about which it did not know, or could not have known. Corfu Channel, I.C.J. Reports 1949, at 18.

[168] On anonymity see Sameer Parekh, Prospects for Remailers: Where is Anonymity Heading on the Internet, First Monday, October, 1996, available at http://www.firstmonday.dk/.

[169] Treaty Between the United States of America and the Swiss Confederation on Mutual Assistance in Criminal Matters, 27 U.S.T. 2019, T.I.A.S. No. 8302 (1977)

[170] Under the U.S. Federal Rules of Civil Procedure, letters rogatory are written communications sent by a court in which a case is pending to a court or judge in a foreign country, requesting that the testimony of a witness residing within the latter court's jurisdiction be taken under that court's local procedures and transmitted to the first court for use in the pending case. Fed. R. Civ. P. 28.

[171] Interpol is an organization, headquartered in Lyon, France, supporting international cooperation and exchange of information among police in over 150 countries. Fenton Bresler, Interpol (1992).

[172] Arguably, though, for purposes of general deterrence, the fact of a response, and its vigor, may be significant, regardless of whether the response is directed toward the proper culprit, especially where the public remains unaware that the actual culprits have escaped punishment. Cf. Jeremy Bentham, Principles of Penal Law, Pt. II, bk. 1, ch. 3, in J. Bentham's Works 396, 402 (J. Bowring ed. 1843) ("When a man supposes pain to be the consequence of an act, he is fed upon in such a manner as tends with a certain force, to withdraw him, as it were, from the commission of the act.") Nevertheless, and not surprisingly, knowingly or willfully attacking foreign official or unofficial targets without a substantive factual basis for such an attack would be unjustified under international law. Case Concerning Military and Paramilitary Activities in and Against Nicaragua, (Nicaragua v. U.S.), ICJ Reports 1986, 14, 195. Such attacks might violate U.S. law as well. See generally, John Hart Ely, The American War in Indochina, Part II: The Unconstitutionality of the War They Didn't Tell Us About, 42 Stan. L. Rev. 1093 (1990)

[173] Vaughan Lowe, Case and Comment, Lockerbie--Changing the Rules During the Game, 5 Cambridge L.J. 408, 408-410 (1992)

[174] U.S. v. Rauscher, 119 U.S. 407, 411-12 (1886); Factor v. Laubenheimer, 290 U.S. 276, 287 (1933). Indeed, under U.S. law the United States may not extradite a citizen in the absence of a statute or treaty obligation. 18 U.S.C. Sec. 3194; Valentine v. U.S. ex. rel. Neidecker, 299 U.S. 5, 8-9 (1936); See also U.S. v. Alvarez-Machain, 504 U.S. 655 (1992); Barry Carter & Philip Trimble, International Law 813-14 (2d ed. 1995).

[175] For example, the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation provides a basis for extradition among its signatories only for offenses related to the goal enunciated in its title.

[176] See, e.g., J. Storke, Introduction to International Law 193-200 (9th ed. 1984); Joyner & Rothbaum, supra note 156, at 235-36.

[177] The subject of jurisdiction over and in cyberspace is now the subject of great scholarly interest, e.g. David R. Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace, 48 Stan. L.R. 1367 (1996); William S. Byassee, Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community, 30 Wake Forest L.R. 197 (1995); Henry H. Perritt, Jr., Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction, University of Oslo, October 12, 1995 (available at http://www.law.vill.edu/chron/articles/oslo/oslo12.htm), although the topic does not yet appear to have been examined from a national security perspective.

[178] See The Eisler Extradition Case, 43 Am. J. Int'l L. 487 (England 1949); Henkin, Pugh, et al., supra note 138 at 1112.

[179] Who Stops the Hacker? KIJK (Netherlands), May 1995, at 22-25.

[180] Simson L. Garfinkel, FBI Uses Hackers' Tools to Sniff Out Hacker's Lair, S.J. Mercury News, April 8, 1996 at B1; U.S. Permanent Subcommittee On Investigations, Committee on Governmental Affairs, Appendix "A" to Staff Statement (June 5, 1996) at 7; Bob Drummond, U.S. Uses First Court-Ordered Wiretap on Computer Network, Bloomberg, March 29, 1996.

[181] See Bowman, supra note 148, at 1941.

[182] Joyner & Rothbaum, supra note 156, at 242-45

[183] Marc Weller, Crisis for the New World Order, 142 New L.J. 592 (May 1, 1992).

[184] Joyner & Rothbaum, supra note 156, at 248-49; Henkin, et al., at 1113; Liskofsky, The Abu Daoud Case: Law or Politics, 7 Is. Yb. H. Rtg. 66 (1977).

[185] Joyner & Rothbaum, supra note 156, at 249.

[186] In a different context, the reluctance of some developing countries to provide intellectual property protection for Western pharmaceutical companies' products has frustrated Western countries, as the developing nations hope to benefit from technological advances without paying the profits that the leading technological nations demand.

[187] See, e.g., A. Michael Froomkin, The Internet as a Source of Regulatory Arbitrage, in Borders in Cyberspace, (Brian Kahin and Charles Nesson, eds. 1997)

[188] Clifford Stoll, The Cuckoo's Egg (1989).

[189] L.T. Greenberg & S.E. Goodman, Is Big Brother Hanging By His Bootstraps? 39 Comm. ACM 11, 13 (July 1996); U.S. Dept. of State, Bureau for International Narcotics and Law Enforcement Affairs, International Narcotics Control Strategy Report 496-503, 581-82 (March 1996).

[190] See, e.g., Robert G. Lynch, Do State and Local Tax Incentives Work? (1996); Ian Ayres, Judging Close Corporations in the Age of Statutes, 70 Wash. U.L.Q. 365 (1992)

[191] U.S. v. Alvarez-Machain, 504 U.S. 655 (1992).

[192] Henkin, supra note 17, at 258-260. After the most famous international abduction, when Israeli agents kidnapped Adolf Eichmann from Argentina and brought him to Israel for trial for his role in the Holocaust, Argentina accepted Israel's apology for violation of its sovereignty, but did not request Eichmann's return. Id.

[193] UN Charter, Art. 2(3).

[194] UN Charter, Art. 2(4)

[195] UN Charter, Art. 51.

[196] ICJ Reports 1986, at 195, 232. Although the U.S. did not recognize the authority of the ICJ to adjudicate the case, and Nicaragua has dropped its complaint, the Court's analysis on this point, irrespective of the actual facts of the case, seems consistent with international law.

[197] ICJ Reports 1986, at 195

[198] Feder, supra note 146, at 410-416

[199] The criminal code of West Virginia, for example, sets out a virtual list of the traditional elements of burglary: If any person shall, 1) in the nighttime, 2(a)) break and enter, or enter without breaking, or shall, 2(b)) in the daytime, break and enter, 3) the dwelling house, or an outhouse adjoining thereto or occupied therewith, 4) of another, 5) with intent to commit a crime therein, he shall be deemed guilty of burglary. W. Va. Code § 61-3-11 (1996).

[200] Restatement 3d, The Foreign Relations Law of the United States (1987) sec. 905. See, e.g., George Bunn, Expanding Nuclear Options: Is the U.S. Negating its Non-Use Pledges? Arms Control Today, May/June 1996, at 7, 9.

[201] The humanitarian consideration is discussed in Part II. B. 2., supra .

[202] See Part II. C. 1., supra.

[203] The comparability of electronic intrusion to physical intrusion is not unquestionable, though, and it is not inappropriate to use publicly available neutral communications facilities for belligerent communications. See Part II. B. 1., supra.

[204] Of course, if the initial attack is considered an "armed attack," the argument that it is somehow distinct from actual force, and that therefore a conventional military response would be disproportionate, would seem strained.

[205] Feder, supra note 146, at, 403-04. As an American professor who later became a Judge of the International Court of Justice stated, "the right of self defense, by its very nature must escape legal regulation." Philip C. Jessup, A Modern Law of Nations 163. Historically, the U.S. government has taken a broad view of self defense. During the negotiations for the 1928 Kellogg-Briand treaty, the U.S. argued that each nation "is free at all times and regardless of treaty provisions to defend its territory from attack or invasion and it alone is competent to decide whether circumstances require recourse to war or peace." Robert F. Turner, Covert Action and the Law, 20 Yale J. Int'l L. 427, 433 & n.34 (1995). Furthermore, the language of Article 51 mentions "inherent" rights, although the U.S. has been skeptical of some nations' assertion of inherent rights to respond militarily to activities other than "armed attack." Feder, supra note 146, at 403-04.

[206] As Emmet Paige, Assistant Secretary of Defense for Command, Control, Communications and intelligence, reportedly said in 1995, "We have an offensive capability, but we can't discuss it. . . . [However] you'd feel good if you knew about it."

Neil Munro, Pentagon Developing Cyberspace Weapons, Washington Technology, (June 22, 1995).

[207] Given the predisposition of the United Nations, it would seem that the U.S. should only pursue a declaration regarding information warfare if it wants to limit its use, as the majority of other nations seem likely to fear U.S. capabilities

[208] Henkin, supra note 17 at 37-38. See also, generally, Charney, supra note 22.

[209] Such treaties included: the Tokyo Convention on Offenses and Certain Other Acts Committed Against on Board Aircraft (1963); the Hague Convention for the Suppression of Unlawful Seizure of Aircraft (1970); and the Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation (1973).

[210] The Convention's coverage would thus seem to apply to many new information attacks against aircraft or the air traffic control system.

[211] Between the provisions of the Montreal Convention and the structures of the International Civil Aviation Organization (ICAO), it is likely that the air traffic control system has significant legal protections. Intentional destruction of civil aircraft in flight is generally illegal, whether conducted with information technology or explosives, and states have an obligation to extradite or try the perpetrators of acts. The adequacy of physical and technological protections of the air traffic control system is, of course, another matter and is beyond the scope of this report.

[212] Advisory Opinion 58-63

[213] The possible applicability of arms control for information warfare is discussed in David Elliott, Lawrence Greenberg, and Kevin Soo Hoo, Strategic Information Warfare: A New Arena for Arms Control? (1997)

[214] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and Their Destruction, (1972); Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases, and of Bacteriological Methods of Warfare (1925).

[215] Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (1977)

[216] Protocol on Blinding Laser Weapons (1995); Burrus M. Carnahan & Marjorie Robertson, Current Developments, The Protocol on "Blinding Laser Weapons": A New Direction for International Humanitarian Law, 90 Am. J. Int'l L. 484 (1996).